

JP 99/05689

14.10.99

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 29 OCT 1999	
WIPO	PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

1999年 4月 9日

出願番号
Application Number:

平成11年特許願第103337号

出願人
Applicant(s):

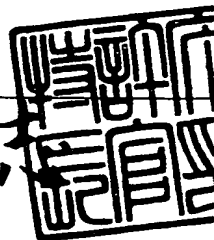
ソニー株式会社

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a)OR(b)

1999年 8月24日

特許庁長官
Commissioner,
Patent Office

平佐山建



出証番号 出証特平11-30

特平 11-103337

【書類名】 特許願
【整理番号】 9900015013
【提出日】 平成11年 4月 9日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 12/16
【発明者】
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社

内
松山 科子

【氏名】
【発明者】
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社

内
石橋 義人

【氏名】
【発明者】
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社

内
浅野 智之

【氏名】
【発明者】
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社

内
北村 出

【氏名】
【発明者】
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社

内
北原 淳

【特許出願人】
【識別番号】 000002185
【氏名又は名称】 ソニー株式会社
【代表者】 出井 伸之

出証特平 11-30591

特平 11-103337

【代理人】

【識別番号】 100082131

【弁理士】

【氏名又は名称】 稲本 義雄

【電話番号】 03-3369-6479

【先の出願に基づく優先権主張】

【出願番号】 平成10年特許願第293829号

【出願日】 平成10年10月15日

【手数料の表示】

【予納台帳番号】 032089

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 管理装置および方法、情報処理装置および方法、提供媒体、並びに情報利用システム

【特許請求の範囲】

【請求項1】 暗号化された情報を提供する情報提供装置、および前記情報を利用する情報処理装置を管理する管理装置において、

前記情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、前記情報処理装置のIDを基に、前記情報処理装置を登録する登録手段を備えることを特徴とする管理装置。

【請求項2】 前記データは、前記IDに対応して決済の可否を示すデータを含む

ことを特徴とする請求項1に記載の管理装置。

【請求項3】 前記登録手段は、前記管理装置と通信する前記情報処理装置に従属する他の情報処理装置を登録することを特徴とする請求項1に記載の管理装置。

【請求項4】 暗号化された情報を提供する情報提供装置、および前記情報を利用する情報処理装置を管理する管理方法において、前記情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、前記情報処理装置のIDを基に、前記情報処理装置を登録する登録ステップを含むことを特徴とする管理方法。

【請求項5】 暗号化された情報を提供する情報提供装置、および前記情報を利用する情報処理装置を管理する管理装置に、前記情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、前記情報処理装置のIDを基に、前記情報処理装置を登録する登録ステップを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項6】 管理装置に登録され、情報提供装置から提供される暗号化された情報を利用する情報処理装置において、

前記情報処理装置に従属する他の情報処理装置の登録を請求する登録請求手段

を備えることを特徴とする情報処理装置。

【請求項 7】 前記情報処理装置は、前記情報処理装置に従属する他の情報処理装置の決済処理を代行する決済代行手段

を更に備えることを特徴とする請求項 6 に記載の情報処理装置。

【請求項 8】 管理装置に登録され、情報提供装置から提供される暗号化された情報を利用する情報処理装置の情報処理方法において、

前記情報処理装置に従属する他の情報処理装置の登録を請求する登録請求ステップ

を含むことを特徴とする情報処理方法。

【請求項 9】 管理装置に登録され、情報提供装置から提供される暗号化された情報を利用する情報処理装置に、

前記情報処理装置に従属する他の情報処理装置の登録を請求する登録請求ステップ

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項 10】 暗号化されて提供される情報を復号し、利用する情報処理装置、および前記情報処理装置を管理する管理装置からなる情報利用システムにおいて、

前記管理装置は、

前記情報処理装置の ID およびその ID に対応して登録の可否を示すデータを有し、前記情報処理装置の ID を基に、前記情報処理装置に登録する登録手段を備え、

前記情報処理装置は、

前記情報処理装置に従属する他の情報処理装置の登録を請求する登録請求手段

を備えることを特徴とする情報利用システム。

【請求項 11】 管理装置に管理され、かつ、他の情報処理装置と接続され、暗号化された情報を復号し、利用する情報処理装置において、

前記管理装置および前記他の情報処理装置と相互認証する相互認証手段と、

所定の情報を復号する復号化手段と、
 前記管理装置により作成された登録条件を授受する授受手段と、
 前記授受手段により授受された前記登録条件を記憶する記憶手段と、
 前記記憶手段により記憶されている前記登録条件に基づいて、動作を制御する
 制御手段と
 を備えることを特徴とする情報処理装置。

【請求項 12】 管理装置に管理され、かつ、他の情報処理装置と接続され、
 暗号化された情報を復号し、利用する情報処理装置の情報処理方法において、
 前記管理装置および前記他の情報処理装置と相互認証する相互認証ステップと

所定の情報を復号する復号化ステップと、
 前記管理装置により作成された登録条件を授受する授受ステップと、
 前記授受ステップで授受された前記登録条件を記憶する記憶ステップと、
 前記記憶ステップで記憶された前記登録条件に基づいて、動作を制御する制御
 ステップと
 を含むことを特徴とする情報処理方法。

【請求項 13】 管理装置に管理され、かつ、他の情報処理装置と接続され、
 暗号化された情報を復号し、利用する情報処理装置に、
 前記管理装置および前記他の情報処理装置と相互認証する相互認証ステップと

所定の情報を復号する復号化ステップと、
 前記管理装置により作成された登録条件を授受する授受ステップと、
 前記授受ステップで授受された前記登録条件を記憶する記憶ステップと、
 前記記憶ステップで記憶された前記登録条件に基づいて、動作を制御する制御
 ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供する
 ことを特徴とする提供媒体。

【請求項 14】 暗号化された情報を復号し、利用する情報処理装置を管理
 する管理装置において、

前記情報処理装置に供給するデータを暗号化する暗号手段と、
 前記情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行手段と、
 前記実行手段により所定の処理を実行するとき、前記情報処理装置の登録条件を作成する作成手段と、
 前記作成手段により作成された前記登録条件を前記情報処理装置に送信する送信手段と
 を備えることを特徴とする管理装置。

【請求項 15】 暗号化された情報を復号し、利用する情報処理装置を管理する管理装置の管理方法において、
 前記情報処理装置に供給するデータを暗号化する暗号ステップと、
 前記情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行ステップと、
 前記実行ステップで所定の処理を実行するとき、前記情報処理装置の登録条件を作成する作成ステップと、
 前記作成ステップで作成された前記登録条件を前記情報処理装置に送信する送信ステップと
 を含むことを特徴とする管理方法。

【請求項 16】 暗号化された情報を復号し、利用する情報処理装置を管理する管理装置に、
 前記情報処理装置に供給するデータを暗号化する暗号ステップと、
 前記情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行ステップと、
 前記実行ステップで所定の処理を実行するとき、前記情報処理装置の登録条件を作成する作成ステップと、
 前記作成ステップで作成された前記登録条件を前記情報処理装置に送信する送信ステップと
 を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、管理装置および方法、情報処理装置および方法、提供媒体、並びに情報利用システムに関し、特に、暗号化された情報を復号する管理装置および方法、情報処理装置および方法、提供媒体、並びに情報利用システムに関する。

【0002】

【従来技術】

音楽などの情報を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザは、その情報処理装置で情報を復号して、再生するシステムがある。ユーザは、複数の情報処理装置で、情報を受信し、利用することができる。

【0003】

【発明が解決しようとする課題】

ユーザは、契約のために、所定の手続をせねばならず、情報の提供者は、契約を要求するユーザの契約の可否を調査しなければならず、手間がかかり、契約成立までに時間がかかる課題があった。また、情報の提供者は、契約したユーザが不正を行った場合、それを発見するのが困難である課題があった。

【0004】

また、複数の情報処理装置を有するユーザは、それぞれの情報処理装置毎に、契約し、利用料金を精算しなければならず、手間がかかる課題があった。

【0005】

本発明はこのような状況に鑑みてなされたものであり、ユーザが簡単に情報提供の契約ができ、提供者も迅速にユーザの契約の可否が判断できることができるとともに、契約したユーザの不正行為や授受される情報の正当性を容易に確認することができるようにすることを目的とする。

【0006】

【課題を解決するための手段】

請求項 1 に記載の管理装置は、情報処理装置の ID およびその ID に対応して登録の可否を示すデータを有し、情報処理装置の ID を基に、情報処理装置を登録する

登録手段を備えることを特徴とする。

【0007】

請求項4に記載の管理方法は、情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録する登録ステップを含むことを特徴とする。

【0008】

請求項5に記載の提供媒体は、管理装置に、情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録する登録ステップを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0009】

請求項6に記載の情報処理装置は、情報処理装置に従属する他の情報処理装置の登録を請求する登録請求手段を備えることを特徴とする。

【0010】

請求項8に記載の情報処理方法は、情報処理装置に従属する他の情報処理装置の登録を請求する登録請求ステップを含むことを特徴とする。

【0011】

請求項9に記載の提供媒体は、情報処理装置に、情報処理装置に従属する他の情報処理装置の登録を請求する登録請求ステップを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0012】

請求項10に記載のシステムは、管理装置が、情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録する登録手段を備え、情報処理装置が、情報処理装置に従属する他の情報処理装置の登録を請求する登録請求手段を備えることを特徴とする。

【0013】

請求項1に記載の管理装置、請求項4に記載の管理方法、および請求項5に記載の提供媒体においては、情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録する。

【0014】

請求項 6 に記載の情報処理装置、請求項 8 に記載の情報処理方法、および請求項 9 に記載の提供媒体においては、情報処理装置に従属する他の情報処理装置の登録を請求する。

【0015】

請求項 10 に記載のシステムにおいては、管理装置が、情報処理装置の ID およびその ID に対応して登録の可否を示すデータを有し、情報処理装置の ID を基に、情報処理装置を登録し、情報処理装置が、情報処理装置に従属する他の情報処理装置の登録を請求する。

【0016】

請求項 11 に記載の情報処理装置は、管理装置および他の情報処理装置と相互認証する相互認証手段と、所定の情報を復号する復号化手段と、管理装置により作成された登録条件を授受する授受手段と、授受手段により授受された登録条件を記憶する記憶手段と、記憶手段により記憶されている登録条件に基づいて、動作を制御する制御手段とを備えることを特徴とする。

【0017】

請求項 12 に記載の情報処理方法は、管理装置および他の情報処理装置と相互認証する相互認証ステップと、所定の情報を復号する復号化ステップと、管理装置により作成された登録条件を授受する授受ステップと、授受ステップで授受された登録条件を記憶する記憶ステップと、記憶ステップで記憶された登録条件に基づいて、動作を制御する制御ステップとを含むことを特徴とする。

【0018】

請求項 13 に記載の提供媒体は、管理装置および他の情報処理装置と相互認証する相互認証ステップと、所定の情報を復号する復号化ステップと、管理装置により作成された登録条件を授受する授受ステップと、授受ステップで授受された登録条件を記憶する記憶ステップと、記憶ステップで記憶された登録条件に基づいて、動作を制御する制御ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0019】

請求項 1 1 に記載の情報処理装置、請求項 1 2 に記載の情報処理方法、および請求項 1 3 に記載の提供媒体においては、管理装置および他の情報処理装置と相互認証され、所定の情報が暗号化され、管理装置により作成された登録条件が授受され、授受された登録条件が記憶され、記憶された登録条件に基づいて、動作が制御される。

【0020】

請求項 1 4 に記載の管理装置は、情報処理装置に供給するデータを暗号化する暗号手段と、情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行手段と、実行手段により所定の処理を実行するとき、情報処理装置の登録条件を作成する作成手段と、作成手段により作成された登録条件を情報処理装置に送信する送信手段とを備えることを特徴とする。

【0021】

請求項 1 5 に記載の管理方法は、情報処理装置に供給するデータを暗号化する暗号ステップと、情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行ステップと、実行ステップで所定の処理を実行するとき、情報処理装置の登録条件を作成する作成ステップと、作成ステップで作成された登録条件を情報処理装置に送信する送信ステップとを含むことを特徴とする。

【0022】

請求項 1 6 に記載の提供媒体は、情報処理装置に供給するデータを暗号化する暗号ステップと、情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行ステップと、実行ステップで所定の処理を実行するとき、情報処理装置の登録条件を作成する作成ステップと、作成ステップで作成された登録条件を情報処理装置に送信する送信ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0023】

請求項 1 4 に記載の管理装置、請求項 1 5 に記載の管理方法、および請求項 1 6 に記載の提供媒体においては、情報処理装置に供給するデータが復され、情報処理装置から、登録条件が送信されてきたとき、所定の処理が実行され、所定の処理が実行されるとき、情報処理装置の登録条件が作成され、作成された登録条

件が情報処理装置に送信される。

【0024】

【発明の実施の形態】

以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【0025】

図1は、本発明を適用したEMD(Electronic Music Distribution:電子音楽配信)システムを説明する図である。このシステムでユーザに配信されるコンテンツ(Content)とは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。EMDサービスセンタ1は、コンテンツプロバイダ2、ユーザホームネットワーク5等に配送用鍵Kdを送信し、ユーザホームネットワーク5から、コンテンツの利用に応じた課金情報等を受信し、利用料金を精算し、コンテンツプロバイダ2およびサービスプロバイダ3への利益分配の処理を行う。

【0026】

コンテンツプロバイダ2は、デジタル化されたコンテンツを有し、自己のコンテンツであることを証明するためのウォーターマーク（電子透かし）をコンテンツに挿入し、コンテンツを圧縮し、および暗号化し、所定の情報を付加して、サービスプロバイダ3に送信する。

【0027】

サービスプロバイダ3は、専用のケーブルネットワーク、インターネット、または衛星などから構成されるネットワーク4を介して、コンテンツプロバイダ2から供給されたコンテンツに価格を付して、ユーザホームネットワーク5に送信する。

【0028】

ユーザホームネットワーク5は、サービスプロバイダ3から価格を付して送付

されたコンテンツを入手し、コンテンツを復号、再生して利用するとともに課金処理を実行する。課金処理により得られた課金情報は、ユーザホームネットワーク 5 が配送用鍵 K d を EMD サービスセンタ 1 から入手する際、EMD サービスセンタ 1 に送信される。

【0029】

図 2 は、EMD サービスセンタ 1 の機能の構成を示すブロック図である。サービスプロバイダ管理部 11 は、サービスプロバイダ 3 に利益分配の情報を供給するとともに、コンテンツプロバイダ 2 から供給されるコンテンツに付される情報（取扱方針）が暗号化されている場合、サービスプロバイダ 3 に配送用鍵 K d を送信する。コンテンツプロバイダ管理部 12 は、コンテンツプロバイダ 2 に配送用鍵 K d を送信するとともに、利益分配の情報を供給する。著作権管理部 13 は、ユーザホームネットワーク 5 のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC (Japanese Society for Rights of Authors, Composers and Publishers: 日本音楽著作権協会) に送信する。鍵サーバ 14 は、配送用鍵 K d を記憶しており、コンテンツプロバイダ管理部 12、またはユーザ管理部 18 等を介して、配送用鍵 K d をコンテンツプロバイダ 2、またはユーザホームネットワーク 5 等に供給する。ユーザ管理部 18 は、ユーザホームネットワーク 5 のコンテンツの利用の実績を示す情報である課金情報、そのコンテンツに対応する価格情報、およびそのコンテンツに対応する取扱方針を入力し、経歴データ管理部 15 に記憶させる。

【0030】

EMD サービスセンタ 1 からコンテンツプロバイダ 2 およびユーザホームネットワーク 5 を構成するレシーバ 51（図 10 で後述する）への、配送用鍵 K d の定期的な送信の例について、図 3 乃至図 6 を参照に説明する。図 3 は、コンテンツプロバイダ 2 がコンテンツの提供を開始し、ユーザホームネットワーク 5 を構成するレシーバ 51 がコンテンツの利用を開始する、1998 年 1 月における、EMD サービスセンタ 1 が有する配送用鍵 K d、コンテンツプロバイダ 2 が有する配送用鍵 K d、およびレシーバ 51 が有する配送用鍵 K d を示す図である。

【0031】

図3の例において、配送用鍵Kdは、暦の月の初日から月の末日まで、使用可能であり、たとえば、所定のビット数の乱数である”aaaaaaa”の値を有するバージョン1である配送用鍵Kdは、1998年1月1日から1998年1月31日まで使用可能（すなわち、1998年1月1日から1998年1月31日の期間にサービスプロバイダ3がユーザホームネットワーク5に配布するコンテンツを暗号化するコンテンツ鍵Kcoは、バージョン1である配送用鍵Kdで暗号化されている）であり、所定のビット数の乱数である”bbbbbbb”の値を有するバージョン2である配送用鍵Kdは、1998年2月1日から1998年2月28日まで使用可能（すなわち、その期間にサービスプロバイダ3がユーザホームネットワーク5に配布するコンテンツを暗号化するコンテンツ鍵Kcoは、バージョン2である配送用鍵Kdで暗号化されている）である。同様に、バージョン3である配送用鍵Kdは、1998年3月中に使用可能であり、バージョン4である配送用鍵Kdは、1998年4月中に使用可能であり、バージョン5である配送用鍵Kdは、1998年5月中に使用可能であり、バージョン6である配送用鍵Kdは、1998年6月中に使用可能である。

【0032】

コンテンツプロバイダ2がコンテンツの提供を開始するに先立ち、EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年1月から1998年6月まで利用可能な、バージョン1乃至バージョン6の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、記憶する。6月分の配送用鍵Kdを記憶するのは、コンテンツプロバイダ2は、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

【0033】

また、レシーバ51がコンテンツの利用を開始するに先立ち、EMDサービスセンタ1は、レシーバ51に、1998年1月から1998年3月まで、利用可能なバージョン1乃至バージョン3である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、記憶する。3月分の配送用鍵Kdを記憶するのは、レシーバ51が、EMDサービスセンタ1に接続できないなどのトラブル

ルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、EMDサービスセンタ1への接続の頻度を低くし、ユーザホームネットワーク5の負荷を低減するためである。

【0034】

1998年1月1日から1998年1月31日の期間には、バージョン1である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0035】

1998年2月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図4で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年2月から1998年7月まで利用可能な、バージョン2乃至バージョン7の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年2月から1998年4月まで、利用可能なバージョン2乃至バージョン4である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵Kdをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵Kdを利用できるようにするためである。

【0036】

1998年2月1日から1998年2月28日の期間には、バージョン2である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0037】

1998年3月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図5で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年3月から1998年8月

まで利用可能な、バージョン3乃至バージョン8の6つの配送用鍵K dを送信し、コンテンツプロバイダ2は、6つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年3月から1998年5月まで、利用可能なバージョン3乃至バージョン5である3つの配送用鍵K dを送信し、レシーバ51は、3つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵K dおよびバージョン2である配送用鍵K dをそのまま記憶する。

【0038】

1998年3月1日から1998年3月31日の期間には、バージョン3である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0039】

1998年4月1日における、EMDサービスセンタ1の配送用鍵K dのコンテンツプロバイダ2、およびレシーバ51への送信を図6で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年4月から1998年9月まで利用可能な、バージョン4乃至バージョン9の6つの配送用鍵K dを送信し、コンテンツプロバイダ2は、6つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年4月から1998年6月まで、利用可能なバージョン4乃至バージョン6である3つの配送用鍵K dを送信し、レシーバ51は、3つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵K d、バージョン2である配送用鍵K d、およびバージョン3である配送用鍵K dをそのまま記憶する。

【0040】

1998年4月1日から1998年4月30日の期間には、バージョン4である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホ

ームネットワーク 5 を構成する レシーバ 5 1 で利用される。

【0041】

このように、あらかじめ先の月の配送用鍵 K d を配布しておくことで、仮にユーザーが 1, 2 ヶ月まったくセンターにアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、センターにアクセスして鍵を受信することができる。

【0042】

利益分配部 1 6 は、経歴データ管理部 1 5 から供給された、課金情報、価格情報、および取扱方針に基づき、EMD サービスセンタ 1、コンテンツプロバイダ 2、およびサービスプロバイダ 3 の利益を算出する。相互認証部 1 7 は、コンテンツプロバイダ 2、サービスプロバイダ 3、およびユーザホームネットワーク 5 の所定の機器と後述する相互認証を実行する。

【0043】

ユーザ管理部 1 8 は、ユーザ登録データベースを有し、ユーザホームネットワーク 5 の機器から登録の要求があったとき、ユーザ登録データベースを検索し、その記録内容に応じて、その機器を登録したり、または登録を拒絶する等の処理を実行する。ユーザホームネットワーク 5 が EMD サービスセンタ 1 と接続が可能な機能を有する複数の機器から構成されているとき、ユーザ管理部 1 8 は、登録が可能か否かの判定の処理の結果に対応して、決済をする機器を指定し、さらに、コンテンツの利用条件を規定した登録リストをユーザホームネットワーク 5 の所定の機器に送信する。

【0044】

図 7 に示すユーザ登録データベースの例は、ユーザホームネットワーク 5 の機器の機器固有の 64 ビットからなる ID (Identification Data) を記録し、その ID に対応して (すなわち、その ID を有する機器毎に)、決済処理が可能か否か、登録が可能か否か、EMD サービスセンタ 1 と接続が可能か否か等の情報を記録する。ユーザ登録データベースに記録された登録が可能か否かの情報は、決済機関 (例えば、銀行)、またはサービスプロバイダ 3 などから供給される料金の未払い、不正処理等の情報を基に、所定の時間間隔で更新される。登録が不可と記録

されたIDを有する機器の登録の要求に対して、ユーザ管理部18は、その登録を拒否し、登録を拒否された機器は、以後、このシステムのコンテンツを利用できない。

【0045】

ユーザ登録データベースに記録された決済処理が可能か否かの情報は、その機器が、決済可能か否かを示す。ユーザホームネットワーク5が、コンテンツの再生またはコピーなどの利用が可能な複数の機器で構成されているとき、その中の決済処理が可能である1台の機器は、EMDサービスセンタ1に、ユーザホームネットワーク5のEMDサービスセンタ1に登録されている全ての機器の、課金情報、価格情報、および取扱方針を出力する。ユーザ登録データベースに記録されたEMDサービスセンタ1と接続が可能か否かの情報は、その機器が、EMDサービスセンタ1と接続が可能であるか否かを示し、接続ができないと記録された機器は、ユーザホームネットワーク5の他の機器を介して、EMDサービスセンタ1に、課金情報等を出力する。

【0046】

また、ユーザ管理部18は、ユーザホームネットワーク5の機器から課金情報、価格情報、および取扱方針が供給され、その情報を経歴データ管理部15に出力し、さらに、所定の処理（タイミング）で、ユーザホームネットワーク5の機器に、配送用鍵Kdを供給する。

【0047】

課金請求部19は、経歴データ管理部15から供給された、課金情報、価格情報、および取扱方針に基づき、ユーザへの課金を算出し、その結果を、出納部20に供給する。出納部20は、ユーザ、コンテンツプロバイダ2、およびサービスプロバイダ3への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。監査部21は、ユーザホームネットワーク5の機器から供給された課金情報、価格情報、および取扱方針の正当性（すなわち、不正をしていないか）を監査する。

【0048】

図8は、コンテンツプロバイダ2の機能の構成を示すブロック図である。コン

テンツサーバ 31 は、ユーザに供給するコンテンツを記憶し、ウォーターマーク付加部 32 に供給する。ウォーターマーク付加部 32 は、コンテンツサーバ 31 から供給されたコンテンツにウォーターマークを付加し、圧縮部 33 に供給する。圧縮部 33 は、ウォーターマーク付加部 32 から供給されたコンテンツを、ATRAC2 (Adaptive Transform Acoustic Coding 2) (商標) 等の方式で圧縮し、暗号化部 34 に供給する。暗号化部 34 は、圧縮部 33 で圧縮されたコンテンツを、乱数発生部 35 から供給された乱数を鍵 (以下、この乱数をコンテンツ鍵 K_c と称する) として、DES (Data Encryption Standard) などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

【0049】

乱数発生部 35 は、コンテンツ鍵 K_c となる所定のビット数の乱数を暗号化部 34 および暗号化部 36 に供給する。暗号化部 36 は、コンテンツ鍵 K_c を EMD サービスセンタ 1 から供給された配送用鍵 K_d を使用して、DES などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

【0050】

DES は、56 ビットの共通鍵を用い、平文の 64 ビットを 1 ブロックとして処理する暗号方式である。DES の処理は、平文を攪拌し、暗号文に変換する部分 (データ攪拌部) と、データ攪拌部で使用する鍵 (拡大鍵) を共通鍵から生成する部分 (鍵処理部) からなる。DES のすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

【0051】

まず、平文の 64 ビットは、上位 32 ビットの H_0 、および下位 32 ビットの L_0 に分割される。鍵処理部から供給された 48 ビットの拡大鍵 K_1 、および下位 32 ビットの L_0 を入力とし、下位 32 ビットの L_0 を攪拌した F 関数の出力が算出される。F 関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の 2 種類の基本変換から構成されている。次に、上位 32 ビットの H_0 と、F 関数の出力が排他的論理和され、その結果は L_1 とされる。 L_0 は、 H_1 とされる。

【0052】

上位 32 ビットの H_0 および下位 32 ビットの L_0 を基に、以上の処理を 16 回繰り返し、得られた上位 32 ビットの H_{16} および下位 32 ビットの L_{16} が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

【0053】

ポリシー記憶部 37 は、コンテンツの取扱方針（ポリシー）を記憶し、暗号化されるコンテンツに対応して、取扱方針をセキュアコンテナ作成部 38 に出力する。セキュアコンテナ作成部 38 は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 K_{co} 、取扱方針、並びに暗号化されたコンテンツ、暗号化されたコンテンツ鍵 K_{co} 、および取扱方針のハッシュ値をとり作成された署名、さらにコンテンツプロバイダ 2 の公開鍵 K_{pcp} を含む証明書から構成されるコンテンツプロバイダセキュアコンテナを作成し、サービスプロバイダ 3 に供給する。相互認証部 39 は、EMD サービスセンタ 1 から配送用鍵 K_d の供給を受けるのに先立ち、EMD サービスセンタ 1 と相互認証し、また、サービスプロバイダ 3 へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ 3 と相互認証する。

【0054】

署名は、データまたは後述する証明書に付け、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

【0055】

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの 1 ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

【0056】

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その

結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD4, MD5, SHA-1などが用いられる。

【0057】

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

【0058】

公開鍵暗号の中で代表的なRSA (Rivest-Shamir-Adleman) 暗号を、簡単に説明する。まず、2つの十分に大きな素数である p および q を求め、さらに p と q の積である n を求める。 $(p-1)$ と $(q-1)$ の最小公倍数 L を算出し、更に、3以上 L 未満で、かつ、 L と互いに素な数 e を求める（すなわち、 e と L を共通に割り切れる数は、1のみである）。

【0059】

次に、 L を法とする乗算に関する e の乗法逆元 d を求める。すなわち、 d 、 e 、および L の間には、 $ed=1 \bmod L$ が成立し、 d はユークリッドの互除法で算出できる。このとき、 n と e が公開鍵とされ、 p, q , および d が、秘密鍵とされる。

【0060】

暗号文 C は、平文 M から、式（1）の処理で算出される。

【0061】

$$C = M^e \bmod n \quad (1)$$

暗号文 C は、式（2）の処理で平文 M に、復号される。

【0062】

$$M = C^d \bmod n \quad (2)$$

証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式（3）が成立するからである。

【0 0 6 3】

$$M = C^d = (M^e)^d = M^{(ed)} = \text{mod } n \quad (3)$$

秘密鍵 p と q を知っているならば、公開鍵 e から秘密鍵 d は算出できるが、公開鍵 n の素因数分解が計算量的に困難な程度に公開鍵 n の桁数を大きくすれば、公開鍵 n を知るだけでは、公開鍵 e から秘密鍵 d は計算できず、復号できない。以上のように、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【0 0 6 4】

また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線 $y^2 = x^3 + ax + b$ 上の、ある点を B とする。楕円曲線上の点の加算を定義し、 nB は、 B を n 回加算した結果を表す。同様に、減算も定義する。 B と nB から n を算出することは、困難であることが証明されている。 B と nB を公開鍵とし、 n を秘密鍵とする。乱数 r を用いて、暗号文 $C1$ および $C2$ は、平文 M から、公開鍵で式（4）および式（5）の処理で算出される。

【0 0 6 5】

$$C1 = M + rnB \quad (4)$$

$$C2 = rB \quad (5)$$

暗号文 $C1$ および $C2$ は、式（6）の処理で平文 M に、復号される。

【0 0 6 6】

$$M = C1 - nC2 \quad (6)$$

復号できるのは、秘密鍵 n を有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【0 0 6 7】

図9は、サービスプロバイダ3の機能の構成を示すブロック図である。コンテンツサーバ41は、コンテンツプロバイダ2から供給された、暗号化されているコンテンツを記憶し、セキュアコンテナ作成部44に供給する。値付け部42は

、コンテンツに対応した取扱方針を基に、価格情報を作成し、セキュアコンテナ作成部44に供給する。ポリシー記憶部43は、コンテンツプロバイダ2から供給された、コンテンツの取扱方針を記憶し、セキュアコンテナ作成部44に供給する。相互認証部45は、コンテンツプロバイダ2からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ2と相互認証し、また、ユーザホームネットワーク5へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク5と相互認証する。また、コンテンツプロバイダ2が取扱方針を配送用鍵Kdで暗号化して供給する場合、相互認証部45は、EMDサービスセンタ1から配送用鍵Kdの供給を受け付けるのに先立ち、EMDサービスセンタ1と相互認証する。

【0068】

図10は、ユーザホームネットワーク5の構成を示すブロック図である。レシーバ51は、ネットワーク4を介して、サービスプロバイダ3からコンテンツを含んだサービスプロバイダセキュアコンテナを受信し、コンテンツを復号および伸張し、再生する。

【0069】

通信部61は、ネットワーク4を介してサービスプロバイダ3、またはEMDサービスセンタ1と通信し、所定の情報を受信し、または送信する。SAM(Secure Application Module)62は、サービスプロバイダ3、またはEMDサービスセンタ1と相互認証し、コンテンツの暗号を復号し、またはコンテンツを暗号化し、さらに配送用鍵Kd等を記憶する。伸張部63は、コンテンツの暗号を復号し、ATRAC2方式で伸張し、さらに所定のウォータマークをコンテンツに挿入する。IC(Integrated Circuit)カードインターフェース64は、SAM62からの信号を所定の形式に変更し、レシーバ51に装着されたICカード55に出力し、また、ICカード55からの信号を所定の形式に変更し、SAM62に出力する。

【0070】

サービスプロバイダ3、またはEMDサービスセンタ1と相互認証し、課金処理を実行し、コンテンツ鍵Kcoを復号および暗号化し、さらに使用許諾条件情報等の所定のデータを記憶するSAM62は、相互認証モジュール71、課金モジュ

ール72、記憶モジュール7₃、および復号／暗号化モジュール74から構成される。このSAM62は、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパー性）を有する。

【0071】

相互認証モジュール71は、サービスプロバイダ3、またはEMDサービスセンタ1との相互認証を実行し、必要に応じて、一時鍵Ktemp（セッション鍵）を復号／暗号化モジュール74に供給する。課金処理モジュール72は、サービスプロバイダ3から受信したサービスプロバイダセキュアコンテナに含まれる取扱方針および価格情報（並びに、場合によっては、取扱制御情報）から、使用許諾条件情報および課金情報を生成し、記憶モジュール73またはHDD(Hard Disk Drive)52に出力する。記憶モジュール73は、課金処理モジュール72または復号／暗号化モジュール74から供給された課金情報、および配送用鍵Kd等のデータを記憶し、他の機能ブロックが所定の処理を実行するとき、配送用鍵Kd等のデータを供給する。

【0072】

復号／暗号化モジュール74は、復号ユニット91、乱数発生ユニット92、および暗号化ユニット93から構成される。復号ユニット91は、暗号化されたコンテンツ鍵Kcoを配送用鍵Kdで復号し、暗号化ユニット93に出力する。乱数発生ユニット92は、相互認証時に、所定の桁数の乱数を発生し、必要に応じて一時鍵Ktempを生成し、暗号化ユニット93に出力する。暗号化ユニット93は、復号されたコンテンツ鍵Kcoを、再度、記憶モジュール73に保持された保存用鍵Ksaveで暗号化し、HDD52に出力する。暗号化ユニット93は、コンテンツ鍵Kcoを伸張部63に送信するとき、コンテンツ鍵Kcoを乱数発生ユニット92で生成した一時鍵Ktempで暗号化する。

【0073】

コンテンツを復号し、伸張し、所定のウォータマークを付加する伸張部63は、相互認証モジュール75、復号モジュール76、復号モジュール77、伸張モ

ジュール 78、およびウォータマーク付加モジュール 79 から構成される。相互認証モジュール 75 は、SAM 62 と相互認証し、一時鍵 K_{temp} を復号モジュール 76 に出力する。復号モジュール 76 は、一時鍵 K_{temp} で暗号化されたコンテンツ鍵 K_c を一時鍵 K_{temp} で復号し、復号モジュール 77 に出力する。復号モジュール 77 は、HDD 52 に記録された、保存用鍵 K_{save} で暗号化されているコンテンツを、記憶モジュール 73 に記憶されている保存用鍵 K_{save} でコンテンツ鍵 K_c で復号し、伸張モジュール 78 に出力する。伸張モジュール 78 は、復号されたコンテンツを、更に ATRAC2 等の方式で伸張し、ウォータマーク付加モジュール 79 に出力する。ウォータマーク付加モジュール 79 は、コンテンツにレシーバ 51 を特定する所定のウォータマークを挿入し、レコーダ 53 に出力したり、図示せぬスピーカに出力し、音楽を再生する。

【0074】

HDD 52 は、サービスプロバイダ 3 から供給されたコンテンツを記録する。装着された光ディスク（図示せず）にサービスプロバイダ 3 から供給されたコンテンツを記録し、再生するレコーダ 53 は、記録再生部 65、SAM 66、および伸張部 67 から構成される。記録再生部 65 は、光ディスクが装着され、その光ディスクにコンテンツを記録し、再生する。SAM 66 は、SAM 62 と同じ機能を有し、その説明は省略する。伸張部 67 は、伸張部 63 と同じ機能を有し、その説明は省略する。MD (Mini Disk: 商標) ドライブ 54 は、装着された図示せぬ MD にサービスプロバイダ 3 から供給されたコンテンツを記録し、再生する。

【0075】

IC カード 55 は、レシーバ 51 に装着され、記憶モジュール 73 に記憶された配送用鍵 K_d および機器の ID などの所定のデータを記憶する。例えば、新たなレシーバ 51 を購入し、今まで使用していたレシーバ 51 と入れ替えて使用する場合、まず、ユーザは、IC カード 55 に、今まで使用していたレシーバ 51 の記憶モジュール 73 に記憶されていた配送用鍵 K_d などの所定のデータを記憶させる。次に、ユーザは、その IC カード 55 を新たなレシーバ 51 に装着し、そのレシーバ 51 を操作して、EMD サービスセンタ 1 のユーザ管理部 18 にその新たなレシーバ 51 を登録する。EMD サービスセンタ 1 のユーザ管理部 18 は、IC カード

55に記憶されていたデータ（今まで使用していたレシーバ51のIDなど）を基に、ユーザ管理部18が保持しているデータベースから、ユーザの氏名、使用料の払い込みに使用するクレジットカードの番号などのデータを検索し、そのデータを基に、登録の処理を実行するので、ユーザは、面倒なデータを入力する必要がない。ICカード55は、相互認証モジュール80および記憶モジュール81で構成される。相互認証モジュール80は、SAM62と相互認証する。記憶モジュール81は、ICカードインターフェース64を介して、SAM62から供給されたデータを記憶し、記憶したデータをSAM62に出力する。

【0076】

図11は、ユーザホームネットワーク5の他の構成例を示すブロック図である。この構成のレシーバ51およびレコーダ53は、図10に示した伸張部63および伸張部67を省略した構成を有する。その代わり、レコーダ53に接続されているデコーダ56が、伸張部63または伸張部67と同じ機能を有する。その他の構成は、図10における場合と同様である。

【0077】

コンテンツを復号し、伸張し、ウォータマークを付加するデコーダ56は、相互認証モジュール101、復号モジュール102、復号モジュール103、伸張モジュール104、およびウォータマーク付加モジュール105から構成される。相互認証モジュール101は、SAM62またはSAM66と相互認証し、一時鍵Ktempを復号モジュール102に出力する。復号モジュール102は、SAM62から出力され、一時鍵Ktempで暗号化されたコンテンツ鍵Kcoを一時鍵Ktempで復号し、復号モジュール103に出力する。復号モジュール103は、HDD52に記録されたコンテンツをコンテンツ鍵Kcoで復号し、伸張モジュール104に出力する。伸張モジュール104は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォータマーク付加モジュール105に出力する。ウォータマーク付加モジュール105は、コンテンツにデコーダ56を特定する所定のウォータマークを挿入し、レコーダ53に出力したり、図示せぬスピーカに出力し、音楽を再生する。

【0078】

図12は、EMDサービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の間で送受信される情報を説明する図である。コンテンツプロバイダ2は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Kco、取扱方針、および署名をコンテンツプロバイダセキュアコンテナ（その詳細は図13を参照して後述する）に格納し、さらにコンテンツプロバイダセキュアコンテナにコンテンツプロバイダ2の証明書（その詳細は図14を参照して後述する）を付して、サービスプロバイダ3に送信する。コンテンツプロバイダ2はまた、取扱方針、および署名にコンテンツプロバイダ2の証明書を付して、EMDサービスセンタ1に送信する。

【0079】

サービスプロバイダ3は、受信したコンテンツプロバイダセキュアコンテナに含まれる取扱方針を基に価格情報を生成し、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Kco、取扱方針、価格情報、および署名をサービスプロバイダセキュアコンテナ（その詳細は図15を参照して後述する）に格納し、さらにサービスプロバイダセキュアコンテナにサービスプロバイダ3の証明書（その詳細は図16を参照して後述する）を付して、ユーザホームネットワーク5に送信する。サービスプロバイダ3はまた、価格情報、および署名にサービスプロバイダ3の証明書を付して、EMDサービスセンタ1に送信する。

【0080】

ユーザホームネットワーク5は、受信したサービスプロバイダセキュアコンテナに含まれる取扱方針から使用許諾条件情報を生成し、使用許諾条件情報に沿って、コンテンツを利用する。ユーザホームネットワーク5において、コンテンツ鍵Kcoが復号されると、課金情報が生成される。課金情報は、必要に応じ、所定のタイミングで、暗号化され、取扱方針および価格情報と共に署名が付され、EMDサービスセンタ1に送信される。

【0081】

EMDサービスセンタ1は、課金情報および取扱方針を基に使用料金を算出し、またEMDサービスセンタ1、コンテンツプロバイダ2、およびサービスプロバイダ3それぞれの利益を算出する。EMDサービスセンタ1は、さらに、コンテンツ

プロバイダ2から受信した取扱方針、サービスプロバイダ3から受信した価格情報、並びにユーザホームネットワーク5から受信した課金情報、取扱方針、および価格情報を比較し、サービスプロバイダ3またはユーザホームネットワーク5で取扱方針の改竄または不正な価格の付加等の不正がなかったか否かを監査する。

【0082】

図13は、コンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、取扱方針、および署名を含む。署名は、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、および取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ2の秘密鍵K_{scp}で暗号化したデータである。

【0083】

図14は、コンテンツプロバイダ2の証明書を説明する図である。コンテンツプロバイダ2の証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ2に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ2の名前、コンテンツプロバイダの公開鍵K_{pcp}、並びに署名を含む。署名は、証明書のバージョン番号、認証局がコンテンツプロバイダ2に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ2の名前、並びにコンテンツプロバイダの公開鍵K_{pcp}にハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵K_{sca}で暗号化したデータである。

【0084】

図15は、サービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、取扱方針、コンテンツプロバイダ2により作成された署名、価格情報、および署名を含む。署名は、コン

テンツ鍵 K_{co} で暗号化されたコンテンツ、配送用鍵 K_d で暗号化されたコンテンツ鍵 K_{co} 、取扱方針、コンテンツプロバイダ 2 により作成された署名、および価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ 3 の秘密鍵 K_{ssp} で暗号化したデータである。

【0085】

図 16 は、サービスプロバイダ 3 の証明書を説明する図である。サービスプロバイダ 3 の証明書は、証明書のバージョン番号、認証局がサービスプロバイダ 3 に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ 3 の名前、サービスプロバイダの公開鍵 K_{psp} 、並びに署名を含む。署名は、証明書のバージョン番号、認証局がサービスプロバイダ 3 に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ 3 の名前、サービスプロバイダの公開鍵 K_{psp} にハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵 K_{sca} で暗号化したデータである。

【0086】

図 17 は、取扱方針、価格情報、および使用許諾条件情報を示す図である。コンテンツプロバイダ 2 が有する取扱方針（図 17（A））は、コンテンツ毎に用意され、ユーザホームネットワーク 5 が利用可能な利用内容を示す。例えば、図 17（A）の取り扱い方針は、ユーザホームネットワーク 5 がそのコンテンツを再生およびシングルコピーすることは許可するが、マルチコピーは許可しないことを示す。

【0087】

図 18 は、シングルコピーおよびマルチコピーを説明する図である。マルチコピーは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合において、そのコンテンツから、複数のコピーを作成すると言う。ただし、図 18（A）に示すように、コピーを更にコピーすることはできない（許されない）。シングルコピーは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を

購入した場合において、そのコンテンツから、ただ1つのコピーを作成することを言う。シングルコピーの場合も、図18(B)に示すように、コピーを更にコピーすることはできない(許されない)。

【0088】

サービスプロバイダ3は、図17(B)に示すように、コンテンツプロバイダ2からの取扱方針(図17(A))に価格情報を加える。例えば、図17(B)の価格情報は、そのコンテンツを再生して利用するときの料金が150円で、マルチコピーして利用するときの利用料金が80円であることを示す。図17には、例示しないが、シングルコピーの価格情報は、コピーの1回当たりの使用料金を表し、例えば、3回のコピーの利用では、シングルコピーの使用料金の3倍の料金を支払う。マルチコピーまたはシングルコピーが許可されるコンテンツは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合における、そのコンテンツに限られる。

【0089】

ユーザホームネットワーク5は、サービスプロバイダ3から供給される取扱方針が示すコンテンツの利用可能な利用内容(図17(B))から、ユーザが選択した、利用内容を示す使用許諾条件情報(図17(C))を記憶する。例えば、図17(C)の使用許諾条件情報は、そのコンテンツを再生して使用することができ、シングルコピーおよびマルチコピーができないことを示す。

【0090】

図19は、図17の例と比較してコンテンツプロバイダ2が取扱方針に利益分配の情報を加え、サービスプロバイダ3が価格情報に利益分配の情報を加える場合の、取扱方針および価格情報を説明する図である。図17に示す例に対して、図19の例では、コンテンツプロバイダ2の利益が、コンテンツを再生して利用するとき70円で、マルチコピーして利用するとき40円であることを示す情報が、追加されている(図19(A))。更に、利益分配情報として、サービスプロバイダ3の利益が、コンテンツを再生して利用するとき60円で、マルチコピーして利用するとき30円であることが、追加されている(図19(B))。価格は、図17(A)における場合と同様に、再生が150円、マルチコピーが8

0円とされている。価格（例えば150円）からコンテンツプロバイダ2の利益（例えば70円）およびサービスプロバイダ3の利益（例えば60円）を差し引いた金額（例えば20円）が、EMDサービスセンタ1の利益である。EMDサービスセンタ1は、ユーザホームネットワーク5のコンテンツの利用結果を示す課金情報（図19（C））とともに、ユーザホームネットワーク5を介して、取扱方針、利益分配率、および価格情報を得ることで、コンテンツプロバイダ2、サービスプロバイダ3、およびEMDサービスセンタ1のそれぞれの利益を算出できる。

【0091】

図20は、コンテンツの再生の利用に、複数の形態が設定されているときの取扱方針、価格情報、および使用許諾条件情報を説明する図である。図20（A）の例では、サービスプロバイダ3において、取扱方針および価格情報として、コンテンツの再生利用に、制限のない再生、回数制限（この例の場合、5回）のある再生、および期日制限（この例の場合、1998年12月31日まで）のある再生が設定されている。ユーザが、5回の回数制限のある再生を選択して、コンテンツを利用する場合、コンテンツを受け取り、まだ1度も再生していない状態では、図20（B）に示すように、ユーザホームネットワーク5の使用許諾条件情報の回数制限に対応する値には、“5”が記録されている。この回数制限に対応する値は、ユーザホームネットワーク5において、コンテンツが再生（利用）される度にデクリメントされ、例えば、3回再生された後、その値は、図20（C）に示すように“2”とされる。回数制限に対応する値が、“0”となった場合、ユーザホームネットワーク5は、それ以上、そのコンテンツを再生して利用することができない。

【0092】

図21は、EMDサービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の間で送受信される情報の他の例を説明する図である。図12に示した例に対して、図21の例では、サービスプロバイダ3は、コンテンツプロバイダ2からの取扱方針を基に取扱制御情報を作成する。取扱制御情報は、コンテンツなどと共にサービスプロバイダセキュアコンテナに格納され、ユーザホームネットワーク5に送信され、EMDサービスセンタ

1にも送信される。取扱制御情報は、更に、課金情報および取扱方針と共にユーザホームネットワーク5からEMDサービスセンタ1に送信される。

【0093】

図22は、図21の例の場合のサービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、取扱方針、コンテンツプロバイダ2により生成された署名、取扱制御情報、価格情報、および署名を含む。署名は、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、取扱方針、コンテンツプロバイダ2により生成された署名、取扱制御情報、および価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ3の秘密鍵K_{ssp}で暗号化したデータである。

【0094】

図23は、図21の例の場合における、取扱方針、取扱制御情報、価格情報、及び使用許諾条件の構成を示す図である。図23に示す例の場合、コンテンツプロバイダ2の取扱方針（図23（A））は、そのまま価格情報を付しても、取扱方針と対比して価格情報を参照できる形式を有しない。そこで、サービスプロバイダ3は、その取扱方針を基に、価格情報と対比して価格情報を参照できる形式を有する取扱制御情報を生成し、それに価格情報を付して、ユーザホームネットワーク5に送信する（図23（B））。ユーザホームネットワークでは、送信を受けた情報から使用許諾条件情報（図23（C））を生成する。図23のコンテンツプロバイダ2は、図12の場合に比較し、より小さいデータ量の取扱方針を記録すればよい利点がある。

【0095】

図24は、EMDサービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の間で送受信されるコンテンツおよびコンテンツに付随する情報のさらに他の構成を説明する図である。図21に示した例に対して、図24の例では、取扱方針、取扱制御情報、価格情報、および課金情報は、共通鍵暗号により暗号化され、送信される。図24のシステムは、

図 2 1 の例の場合に比較して、システムの外部からの攻撃に対し、安全性が向上する。

【 0 0 9 6 】

図 2 5 は、図 2 4 の例の場合のコンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵 K_{co} で暗号化されたコンテンツ、配送用鍵 K_d で暗号化されたコンテンツ鍵 K_{co} 、配送用鍵 K_d で暗号化された取扱方針、および署名を含む。署名は、コンテンツ鍵 K_{co} で暗号化されたコンテンツ、配送用鍵 K_d で暗号化されたコンテンツ鍵 K_{co} 、および配送用鍵 K_d で暗号化された取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ 2 の秘密鍵 K_{scp} で暗号化したデータである。

【 0 0 9 7 】

図 2 6 は、図 2 4 の例の場合のサービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵 K_{co} で暗号化されたコンテンツ、配送用鍵 K_d で暗号化されたコンテンツ鍵 K_{co} 、配送用鍵 K_d で暗号化された取扱方針、コンテンツプロバイダ 2 により生成された署名、配送用鍵 K_d で暗号化された取扱制御情報、配送用鍵 K_d で暗号化された価格情報、および署名を含む。署名は、コンテンツ鍵 K_{co} で暗号化されたコンテンツ、配送用鍵 K_d で暗号化されたコンテンツ鍵 K_{co} 、配送用鍵 K_d で暗号化された取扱方針、コンテンツプロバイダ 2 により生成された署名、配送用鍵 K_d で暗号化された取扱制御情報、および配送用鍵 K_d で暗号化された価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ 3 の秘密鍵 K_{ssp} で暗号化したデータである。

【 0 0 9 8 】

図 2 7 は、EMDサービスセンタ 1 が、ユーザホームネットワーク 5 から課金情報を受信するときの動作を説明する図である。~~EMDサービスセンタ 1 と相互認証~~した後、レシーバ 5 1 は、一時鍵 K_{temp} を共有化し、共有化した一時鍵 K_{temp} を用いて課金情報、および取扱方針等を暗号化し、EMDサービスセンタ 1 に送信する。ユーザ管理部 1 8 はこれを受信する。ユーザ管理部 1 8 は、受信し

た課金情報、および取扱方針等を共有化した一時鍵K t e m pで復号化した後、経歴データ管理部15および課金請求部19に送信する。経歴データ管理部15は決済を実行すると判定した場合、受信した課金情報を利益分配部16に送信し、さらに、受信した課金情報および取扱方針等を課金請求部19に送信する。利益分配部16は、コンテンツプロバイダ2、サービスプロバイダ3、およびEMDサービスセンタ1自身に対する請求金額および支払金額を算出する。課金請求部19は、ユーザの支払い金額を算出し、その情報を出納部20に送信する。出納部20は、図示せぬ外部の銀行等と通信し、決算処理を実行する。その際、ユーザの料金の未払い等の情報があれば、それらの情報は、課金請求部19およびユーザ管理部18に送信され、以後のユーザの登録処理時、または配送用鍵K dの送信処理時に参照される。ユーザ管理部18はまた、鍵サーバ14からの配送用鍵K dを一時鍵K t e m pで暗号化しユーザホームネットワーク5に送信する。ユーザホームネットワーク5は、受信した配送用鍵K dを共有化した一時鍵K t e m pで復号した後、配送用鍵K dを必要に応じて更新する。

【0099】

図28は、EMDサービスセンタ1の利益分配処理の動作を説明する図である。経歴データ管理部15は、ユーザのコンテンツの使用実績を示す課金情報、取扱方針、および価格データを利益分配部16に送信する。利益分配部16は、これらの情報を基に、コンテンツプロバイダ2、サービスプロバイダ3、およびEMDサービスセンタ1それぞれの利益を算出し、その結果をサービスプロバイダ管理部11、コンテンツプロバイダ管理部12、出納部20、および著作権管理部13に送信する。出納部20は、図示せぬ外部の銀行等と通信し、決算処理を実行する。サービスプロバイダ管理部11は、サービスプロバイダ3の利益の情報をサービスプロバイダ3に送信する。コンテンツプロバイダ管理部12は、コンテンツプロバイダ2の利益の情報をコンテンツプロバイダ2に送信する。監査部21は、ユーザホームネットワーク5の機器から供給された課金情報、価格情報、および取扱方針の正当性を監査する。

【0100】

図29は、EMDサービスセンタ1の、コンテンツの利用実績の情報をJASRACに

送信する処理の動作を説明する図である。経歴データ管理部 15 は、ユーザのコンテンツの使用実績を示す課金情報を著作権管理部 13 および利益分配部 16 に送信する。利益分配部 16 は、JASRAC に対する請求金額および支払金額を算出し、その情報を出納部 20 に送信する。出納部 20 は、図示せぬ外部の銀行等と通信し、決算処理を実行する。著作権管理部 13 は、ユーザのコンテンツの使用実績を JASRAC に送信する。

【0101】

次に、EMD システムの処理について説明する。図 30 は、このシステムのコンテンツの配布および再生の処理を説明するフローチャートである。ステップ S11 において、EMD サービスセンタ 1 のコンテンツプロバイダ管理部 12 は、コンテンツプロバイダ 2 に配送用鍵 Kd を送信し、コンテンツプロバイダ 2 がこれを受信する。その処理の詳細は、図 32 のフローチャートを参照して後述する。ステップ S12 において、ユーザは、ユーザホームネットワーク 5 の機器（例えば、図 10 のレシーバ 51）を操作し、ユーザホームネットワーク 5 の機器を EMD サービスセンタ 1 のユーザ管理部 18 に登録する。この登録処理の詳細は、図 36 のフローチャートを参照して後述する。ステップ S13 において、EMD サービスセンタ 1 のユーザ管理部 18 は、ユーザホームネットワーク 5 と、図 33 乃至図 35 に示したように相互認証した後、ユーザホームネットワーク 5 の機器に、配送用鍵 Kd を送信する。ユーザホームネットワーク 5 はこの鍵を受信する。この処理の詳細は、図 45 のフローチャートを参照して説明する。

【0102】

ステップ S14 において、コンテンツプロバイダ 2 のセキュアコンテナ作成部 38 は、サービスプロバイダ 3 にコンテンツプロバイダセキュアコンテナを送信する。この送信処理の詳細は、図 47 のフローチャートを参照して後述する。

【0103】

~~ステップ S15 において、サービスプロバイダ 3 のセキュアコンテナ作成部 4~~
4 は、ユーザホームネットワーク 5 からの要求に応じて、ネットワーク 4 を介して、ユーザホームネットワーク 5 にサービスプロバイダセキュアコンテナを送信する。この送信処理の詳細は、図 49 のフローチャートを参照して後述する。な

お、ネットワーク 4 が、衛星通信により構成されている場合、サービスプロバイダセキュアコンテナの要求は、ユーザホームネットワーク 5 からサービスプロバイダ 3 に対して行われたい。

【0104】

ステップ S 16 において、ユーザホームネットワーク 5 の課金モジュール 7 2 は、課金処理を実行する。課金処理の詳細は、図 5 1 のフローチャートを参照して後述する。ステップ S 17 において、ユーザは、ユーザホームネットワーク 5 の機器でコンテンツを再生する。再生処理の詳細は、図 5 2 のフローチャートを参照して後述する。

【0105】

一方、コンテンツプロバイダ 2 が、取扱方針を暗号化して送信する場合の処理は、図 3 1 のフローチャートで示すようになる。ステップ S 2 1 において、EMD サービスセンタ 1 のコンテンツプロバイダ管理部 1 2 は、コンテンツプロバイダ 2 に配送用鍵 K d を送信する。ステップ S 2 2 において、EMD サービスセンタ 1 のサービスプロバイダ管理部 1 1 は、サービスプロバイダ 3 に配送用鍵 K d を送信する。それ以降のステップ S 2 3 乃至ステップ S 2 8 の処理は、図 3 0 のステップ S 1 2 乃至ステップ S 1 7 の処理と同様の処理であり、その説明は省略する。

【0106】

図 3 2 は、図 3 0 のステップ S 1 1 および図 3 1 のステップ S 2 1 に対応する、EMD サービスセンタ 1 がコンテンツプロバイダ 2 へ配送用鍵 K d を送信し、コンテンツプロバイダ 2 がこれを受信する処理の詳細を説明するフローチャートである。ステップ S 3 1 において、EMD サービスセンタ 1 の相互認証部 1 7 は、コンテンツプロバイダ 2 の相互認証部 3 9 と相互認証する。この相互認証処理の詳細は、図 3 3 を参照して後述する。相互認証処理により、コンテンツプロバイダ 2 が、正当なプロバイダであることが確認されたとき、ステップ S 3 2 において、コンテンツプロバイダ 2 の暗号化部 3 4 および暗号化部 3 6 は、EMD サービスセンタ 1 のコンテンツプロバイダ管理部 1 2 から送信された配送用鍵 K d を受信する。ステップ S 3 3 において、コンテンツプロバイダ 2 の暗号化部 3 6 は、受

信した配送用鍵 K_d を記憶する。

【0 1 0 7】

このように、コンテンツプロバイダ 2 は、EMD サービスセンタ 1 から配送用鍵 K_d を受け取る。同様に、図 3 1 に示すフローチャートの処理を行う例の場合、コンテンツプロバイダ 2 以外に、サービスプロバイダ 3 も、図 3 2 と同様の処理で、EMD サービスセンタ 1 から配送用鍵 K_d を受け取る。

【0 1 0 8】

次に、図 3 2 のステップ S 3 1 における、いわゆるなりすましがいないことを確認する相互認証の処理について、1 つの共通鍵を用いる (図 3 3)、2 つの共通鍵を用いる (図 3 4)、および公開鍵暗号を用いる (図 3 5) を例として説明する。

【0 1 0 9】

図 3 3 は、1 つの共通鍵で、共通鍵暗号である DES を用いる、コンテンツプロバイダ 2 の相互認証部 3 9 と EMD サービスセンタ 1 の相互認証部 1 7 との相互認証の動作を説明するフローチャートである。ステップ S 4 1 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、64 ビットの乱数 R_1 を生成する (乱数生成部 3 5 が生成するようにしてもよい)。ステップ S 4 2 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、DES を用いて乱数 R_1 を、予め記憶している共通鍵 K_c で暗号化する (暗号化部 3 6 で暗号化するようにしてもよい)。ステップ S 4 3 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、暗号化された乱数 R_1 を EMD サービスセンタ 1 の相互認証部 1 7 に送信する。

【0 1 1 0】

ステップ S 4 4 において、EMD サービスセンタ 1 の相互認証部 1 7 は、受信した乱数 R_1 を予め記憶している共通鍵 K_c で復号する。ステップ S 4 5 において、EMD サービスセンタ 1 の相互認証部 1 7 は、32 ビットの乱数 R_2 を生成する。ステップ S 4 6 において、EMD サービスセンタ 1 の相互認証部 1 7 は、復号した 64 ビットの乱数 R_1 の下位 32 ビットを乱数 R_2 で入れ替え、接続 $R_1 H \parallel R_2$ を生成する。なお、ここで $R_i H$ は、 R_i の上位ビットを表し、 $A \parallel B$ は、 A と B の接続 (n ビットの A の下位に、 m ビットの B を結合して、 $(n + m)$ ビット)

ットとしたもの)を表す。ステップS47において、EMDサービスセンタ1の相互認証部17は、DESを用いて $R1H \parallel R2$ を共通鍵 Kc で暗号化する。ステップS48において、EMDサービスセンタ1の相互認証部17は、暗号化した $R1H \parallel R2$ をコンテンツプロバイダ2に送信する。

【0111】

ステップS49において、コンテンツプロバイダ2の相互認証部39は、受信した $R1H \parallel R2$ を共通鍵 Kc で復号する。ステップS50において、コンテンツプロバイダ2の相互認証部39は、復号した $R1H \parallel R2$ の上位32ビット $R1H$ を調べ、ステップS41で生成した、乱数 $R1$ の上位32ビット $R1H$ と一致すれば、EMDサービスセンタ1が正当なセンタであることを認証する。生成した乱数 $R1H$ と、受信した $R1H$ が一致しないとき、処理は終了される。両者が一致するとき、ステップS51において、コンテンツプロバイダ2の相互認証部39は、32ビットの乱数 $R3$ を生成する。ステップS52において、コンテンツプロバイダ2の相互認証部39は、受信し、復号した32ビットの乱数 $R2$ を上位に設定し、生成した乱数 $R3$ をその下位に設定し、接続 $R2 \parallel R3$ とする。ステップS53において、コンテンツプロバイダ2の相互認証部39は、DESを用いて接続 $R2 \parallel R3$ を共通鍵 Kc で暗号化する。ステップS54において、コンテンツプロバイダ2の相互認証部39は、暗号化された接続 $R2 \parallel R3$ をEMDサービスセンタ1の相互認証部17に送信する。

【0112】

ステップS55において、EMDサービスセンタ1の相互認証部17は、受信した接続 $R2 \parallel R3$ を共通鍵 Kc で復号する。ステップS56において、EMDサービスセンタ1の相互認証部17は、復号した接続 $R2 \parallel R3$ の上位32ビットを調べ、乱数 $R2$ と一致すれば、コンテンツプロバイダ2を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

【0113】

図34は、2つの共通鍵 $Kc1$ 、 $Kc2$ で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS61にお

いて、コンテンツプロバイダ 2 の相互認証部 39 は、64 ビットの乱数 R 1 を生成する。ステップ S 62 において、コンテンツプロバイダ 2 の相互認証部 39 は、DES を用いて乱数 R 1 を予め記憶している共通鍵 K c 1 で暗号化する。ステップ S 63 において、コンテンツプロバイダ 2 の相互認証部 39 は、暗号化された乱数 R 1 を EMD サービスセンタ 1 に送信する。

【0114】

ステップ S 64 において、EMD サービスセンタ 1 の相互認証部 17 は、受信した乱数 R 1 を予め記憶している共通鍵 K c 1 で復号する。ステップ S 65 において、EMD サービスセンタ 1 の相互認証部 17 は、乱数 R 1 を予め記憶している共通鍵 K c 2 で暗号化する。ステップ S 66 において、EMD サービスセンタ 1 の相互認証部 17 は、64 ビットの乱数 R 2 を生成する。ステップ S 67 において、EMD サービスセンタ 1 の相互認証部 17 は、乱数 R 2 を共通鍵 K c 2 で暗号化する。ステップ S 68 において、EMD サービスセンタ 1 の相互認証部 17 は、暗号化された乱数 R 1 および乱数 R 2 をコンテンツプロバイダ 2 の相互認証部 39 に送信する。

【0115】

ステップ S 69 において、コンテンツプロバイダ 2 の相互認証部 39 は、受信した乱数 R 1 および乱数 R 2 を予め記憶している共通鍵 K c 2 で復号する。ステップ S 70 において、コンテンツプロバイダ 2 の相互認証部 39 は、復号した乱数 R 1 を調べ、ステップ S 61 で生成した乱数 R 1（暗号化する前の乱数 R 1）と一致すれば、EMD サービスセンタ 1 を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップ S 71 において、コンテンツプロバイダ 2 の相互認証部 39 は、復号して得た乱数 R 2 を共通鍵 K c 1 で暗号化する。ステップ S 72 において、コンテンツプロバイダ 2 の相互認証部 39 は、暗号化された乱数 R 2 を EMD サービスセンタ 1 に送信する。

【0116】

ステップ S 73 において、EMD サービスセンタ 1 の相互認証部 17 は、受信した乱数 R 2 を共通鍵 K c 1 で復号する。ステップ S 74 において、EMD サービスセンタ 1 の相互認証部 17 は、復号した乱数 R 2 が、ステップ S 66 で生成した

乱数 R_2 （暗号化する前の乱数 R_2 ）と一致すれば、コンテンツプロバイダ 2 を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

【0117】

図 35 は、公開鍵暗号である、160 ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ 2 の相互認証部 39 と EMD サービスセンタ 1 の相互認証部 17 との相互認証の動作を説明するフローチャートである。ステップ S81 において、コンテンツプロバイダ 2 の相互認証部 39 は、64 ビットの乱数 R_1 を生成する。ステップ S82 において、コンテンツプロバイダ 2 の相互認証部 39 は、自分自身の公開鍵 K_{pcp} を含む証明書（認証局から予め取得しておいたもの）と、乱数 R_1 を EMD サービスセンタ 1 の相互認証部 17 に送信する。

【0118】

ステップ S83 において、EMD サービスセンタ 1 の相互認証部 17 は、受信した証明書の署名（認証局の秘密鍵 K_{sca} で暗号化されている）を、予め取得しておいた認証局の公開鍵 K_{pca} で復号し、コンテンツプロバイダ 2 の公開鍵 K_{pcp} とコンテンツプロバイダ 2 の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ 2 の公開鍵 K_{pcp} およびコンテンツプロバイダ 2 の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵 K_{pcp} およびコンテンツプロバイダ 2 の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ 2 の公開鍵 K_{pcp} およびコンテンツプロバイダ 2 の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵 K_{pcp} が改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

【0119】

適正な認証結果が得られたとき、ステップ S84 において、EMD サービスセンタ 1 の相互認証部 17 は、64 ビットの乱数 R_2 を生成する。ステップ S85 に

において、EMDサービスセンタ1の相互認証部17は、乱数 R_1 および乱数 R_2 の接続 $R_1 \parallel R_2$ を生成する。ステップS86において、EMDサービスセンタ1の相互認証部17は、接続 $R_1 \parallel R_2$ を自分自身の秘密鍵 $K_{se sc}$ で暗号化する。ステップS87において、EMDサービスセンタ1の相互認証部17は、接続 $R_1 \parallel R_2$ を、ステップS83で取得したコンテンツプロバイダ2の公開鍵 $K_{pc p}$ で暗号化する。ステップS88において、EMDサービスセンタ1の相互認証部17は、秘密鍵 $K_{se sc}$ で暗号化された接続 $R_1 \parallel R_2$ 、公開鍵 $K_{pc p}$ で暗号化された接続 $R_1 \parallel R_2$ 、および自分自身の公開鍵 $K_{pe sc}$ を含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ2の相互認証部39に送信する。

【0120】

ステップS89において、コンテンツプロバイダ2の相互認証部39は、受信した証明書の署名を予め取得しておいた認証局の公開鍵 $K_{pc a}$ で復号し、正しければ証明書から公開鍵 $K_{pe sc}$ を取り出す。この場合の処理は、ステップS83における場合と同様であるので、その説明は省略する。ステップS90において、コンテンツプロバイダ2の相互認証部39は、EMDサービスセンタ1の秘密鍵 $K_{se sc}$ で暗号化されている接続 $R_1 \parallel R_2$ を、ステップS89で取得した公開鍵 $K_{pe sc}$ で復号する。ステップS91において、コンテンツプロバイダ2の相互認証部39は、自分自身の公開鍵 $K_{pc p}$ で暗号化されている接続 $R_1 \parallel R_2$ を、自分自身の秘密鍵 $K_{sc p}$ で復号する。ステップS92において、コンテンツプロバイダ2の相互認証部39は、ステップS90で復号された接続 $R_1 \parallel R_2$ と、ステップS91で復号された接続 $R_1 \parallel R_2$ を比較し、一致すればEMDサービスセンタ1を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

【0121】

適正な認証結果が得られたとき、ステップS93において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数 R_3 を生成する。ステップS94において、コンテンツプロバイダ2の相互認証部39は、ステップS90で取得した乱数 R_2 および生成した乱数 R_3 の接続 $R_2 \parallel R_3$ を生成する。ステップS

95において、コンテンツプロバイダ2の相互認証部39は、接続R2 || R3を、ステップS89で取得した公開鍵K_{pesc}で暗号化する。ステップS96において、コンテンツプロバイダ2の相互認証部39は、暗号化した接続R2 || R3をEMDサービスセンタ1の相互認証部17に送信する。

【0122】

ステップS97において、EMDサービスセンタ1の相互認証部17は、暗号化された接続R2 || R3を自分自身の秘密鍵K_{sec}で復号する。ステップS98において、EMDサービスセンタ1の相互認証部17は、復号した乱数R2が、ステップS84で生成した乱数R2（暗号化する前の乱数R2）と一致すれば、コンテンツプロバイダ2を適正なプロバイダとして認証し、一致しなければ、不適正なプロバイダとして、処理を終了する。

【0123】

以上のように、EMDサービスセンタ1の相互認証部17とコンテンツプロバイダ2の相互認証部39は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵K_{temp}として利用される。

【0124】

図36は、図30のステップS12および図31のステップS23に対応する、レシーバ51がEMDサービスセンタ1のユーザ管理部18に登録する処理を説明するフローチャートである。ステップS101において、レシーバ51のSAM62は、ICカードインターフェース64の出力から、レシーバ51にバックアップ用のICカード55が装着されているか否かを判定し、バックアップ用のICカード55が装着されていると判定された場合（例えば、レシーバ51が新たなレシーバ51に変更され、元のレシーバ51のデータを、新たなレシーバ51に引き継ぐために、元のレシーバ51のデータをバックアップ用のICカード55にバックアップさせている場合）、ステップS102に進み、ICカード55に記憶されているバックアップデータの読み込み処理を実行する。この処理の詳細は、図41のフローチャートを参照して後述する。勿論、この読み込み処理が実行されるためには、その前に、ICカード55に、バックアップデータを記憶させる必要があるが、その処理は、図39を参照して後述する。

【0125】

ステップS101において、バックアップ用のICカード55が装着されていないと判定された場合、手続は、ステップS102をスキップし、ステップS103に進む。ステップS103において、SAM62の相互認証モジュール71は、EMDサービスセンタ1の相互認証部17と相互認証し、SAM62は、証明書をEMDサービスセンタ1のユーザ管理部18に送信する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS103で、SAM62がEMDサービスセンタ1のユーザ管理部18に送信する証明書は、図37に示すデータを含む。SAM62が送信する証明書は、図14に示すコンテンツプロバイダ2の証明書とほぼ同様の構成を有するが、更に、他のSAMに従属するか否かを示すデータを含んでいる。ステップS104において、SAM62は、通信部61を介して、一時鍵 K_{temp} で暗号化した、ユーザの銀行等の決済機関の情報等をEMDサービスセンタ1のユーザ管理部18に送信する。

【0126】

ステップS105において、EMDサービスセンタ1のユーザ管理部18は、受信したSAM62のIDを基に、図7に示したユーザ登録データベースを検索する。ステップS106において、EMDサービスセンタ1のユーザ管理部18は、受信したIDを有するSAM62の登録が可能であるか否かを判定し、受信したIDを有するSAM62の登録が可能であると判定された場合、ステップS107に進み、受信したIDを有するSAM62が、新規登録であるか否かを判定する。ステップS107において、受信したIDを有するSAM62が、新規登録ではないと判定された場合、手続は、ステップS108に進む。

【0127】

ステップS108において、EMDサービスセンタ1のユーザ管理部18は、更新登録を実行し、受信したIDを基にユーザ登録データベースを検索し、登録リストを作成する。この登録リストは、例えば、図38に示す構造を有し、機器のSAMのIDに対応して、EMDサービスセンタ1のユーザ管理部18が登録を拒絶したか否かを示す登録拒絶フラグ、従属する機器である場合のコンテンツ鍵 K_{co} の利用条件を示すステータスフラグ、従属する機器であるか否かを示すコンディショ

ンフラグ、並びに登録拒絶フラグ、ステータスフラグ、およびコンディションフラグにハッシュ関数を適用して生成したハッシュ値をEMDサービスセンタ1の秘密鍵K s e s cで暗号化した署名から構成される。

【0128】

機器のSAMのIDは、機器の固有の64ビットからなるIDを示す（図38では、16進数で示す）。登録拒絶フラグの”1”は、EMDサービスセンタ1のユーザ管理部18が対応するIDを有する機器に登録したことを示し、登録拒絶フラグの”0”は、EMDサービスセンタ1のユーザ管理部18が対応するIDを有する機器の登録を拒絶したことを示す。

【0129】

ステータスフラグのMSB(Most Significant Bit)の”1”は、対応するIDを有する子の機器（例えばレコーダ53）が従属した親の機器（例えばレシーバ51）からコンテンツ鍵K c oをもらえることを示し、ステータスフラグのMSBの”0”は、対応するIDを有する子の機器が従属した親の機器からコンテンツ鍵K c oをもらえないことを示している。ステータスフラグの上位から2ビット目の”1”は、対応するIDを有する子の機器が従属した親の機器から、親の機器の保存用鍵K s a v eで暗号化されたコンテンツ鍵K c oをもらえることを示す。ステータスフラグの上位から3ビット目の”1”は、対応するIDを有する子の機器が従属した親の機器から、配送用鍵K dで暗号化されたコンテンツ鍵K c oをもらえることを示す。ステータスフラグのLSB(Least Significant Bit)の”1”は、従属した親の機器が配送用鍵K dで暗号化したコンテンツ鍵K c oを購入し、対応するIDを有する子の機器に、一時鍵K t e m pで暗号化してコンテンツ鍵K c oを渡すことを示す。

【0130】

コンディションフラグの”0”は、対応するIDを有する機器がEMDサービスセンタ1のユーザ管理部18と直接通信が出来る（すなわち、例えばレシーバ51のような親の機器である）ことを示し、コンディションフラグの”1”は、対応するIDを有する機器がEMDサービスセンタ1のユーザ管理部18と直接通信が出来ない（すなわち、例えばレコーダ53のような子の機器である）ことを示す。

コンディションフラグが” 0 ” のとき、ステータスフラグは常に” 0000 ” に設定される。

【0131】

ステップS109において、EMDサービスセンタ1のユーザ管理部18は、相互認証部17から供給された一時鍵K t e m pで暗号化した、鍵サーバ14から供給された配送用鍵K dをレシーバ51のSAM62に送信する。ステップS110において、レシーバ51のSAM62は、受信した配送用鍵K dを一時鍵K t e m pで復号し、記憶モジュール73に記憶させる。

【0132】

ステップS111において、EMDサービスセンタ1のユーザ管理部18は、一時鍵K t e m pで暗号化した登録リストをレシーバ51のSAM62に送信する。ステップS112において、レシーバ51のSAM62は、受信した登録リストを一時鍵K t e m pで復号し、記憶モジュール73に記憶させ、処理は終了する。

【0133】

ステップS107において、受信したIDを有するSAM62が、新規登録であると判定された場合、手続は、ステップS114に進み、EMDサービスセンタ1のユーザ管理部18は、新規登録を実行し、登録リストを作成し、ステップS109に進む。

【0134】

ステップS106において、受信したIDを有するSAM62の登録が不可であると判定された場合、ステップS113に進み、EMDサービスセンタ1のユーザ管理部18は、登録拒絶の登録リストを作成し、ステップS111に進む。

【0135】

このように、レシーバ51は、EMDサービスセンタ1に登録される。

【0136】

次に、今まで使用していたレシーバ51の記憶モジュール73に記憶された配送用鍵K dなどの所定のデータをICカード55に記憶させる処理の詳細を、図39のフローチャートを参照して説明する。ステップS121において、SAM62の相互認証モジュール71は、ICカード55の相互認証モジュール80と相互認

証する。この認証処理は、図 33 乃至図 35 を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップ S122 において、SAM 62 の乱数発生ユニット 92 は、バックアップ鍵 K_{ic} として用いられる乱数を生成する。ステップ S123 において、SAM 62 の暗号化ユニット 93 は、記憶モジュール 73 に記憶されている SAM の ID 番号、保存用鍵 K_{save} 、および HDD 52 の ID を、バックアップ鍵 K_{ic} を用いて暗号化する。ステップ S124 において、SAM 62 の暗号化ユニット 93 は、EMD サービスセンタ 1 の公開鍵 K_{pesc} でバックアップ鍵 K_{ic} を暗号化する（SAM 62 は、EMD サービスセンタ 1 との間の認証処理（図 35 のステップ S89）において、EMD サービスセンタ 1 の公開鍵 K_{pesc} を取得している）。ステップ S125 において、レシーバ 51 の SAM 62 は、IC カードインターフェース 64 を介して、暗号化された SAM の ID 番号、保存用鍵 K_{save} 、および HDD 52 の ID 並びに暗号化されたバックアップ鍵 K_{ic} を IC カード 55 に送信し、記憶モジュール 81 に記憶させる。

【0137】

以上のように、SAM 62 の記憶モジュール 73 に記憶された SAM の ID 番号、保存用鍵 K_{save} 、および HDD 52 の ID は、バックアップ鍵 K_{ic} を用いて暗号化され、EMD サービスセンタ 1 の公開鍵 K_{pesc} を用いて暗号化されたバックアップ鍵 K_{ic} と共に、IC カード 55 の記憶モジュール 81 に記憶される。

【0138】

今まで使用していたレシーバ 51 の記憶モジュール 73 に記憶された配送用鍵 K_d などの所定のデータを IC カード 55 に記憶させる他の処理の例の詳細を、図 40 のフローチャートを参照して説明する。ステップ S131 において、SAM 62 の相互認証モジュール 71 は、IC カード 55 の相互認証モジュール 80 と相互認証する。ステップ S132 において、SAM 62 の暗号化ユニット 93 は、記憶モジュール 73 に記憶されている SAM の ID 番号、保存用鍵 K_{save} 、および HDD 52 の ID を、EMD サービスセンタ 1 の公開鍵 K_{pesc} を用いて暗号化する。ステップ S133 において、レシーバ 51 の SAM 62 は、IC カードインターフェース 64 を介して、暗号化された SAM の ID 番号、保存用鍵 K_{save} 、および HDD 52 の ID を IC カード 55 に送信し、記憶モジュール 81 に記憶させる。

【0139】

図40に示す処理により、図39に示した場合より簡単な処理で、EMDサービスセンタ1の公開鍵K p e s cを用いて暗号化されたSAMのID番号、保存用鍵K s a v e、およびHDD52のIDは、ICカード55の記憶モジュール81に記憶される。

【0140】

このように、ICカード55にバックアップされたデータは、図36のステップS102の処理で、新しいレシーバ51に読み込まれる。図41は、図39に示す処理でバックアップされたデータを読み出す場合の処理を説明するフローチャートである。ステップS141において、新しいレシーバ51のSAM62の相互認証モジュール71は、ICカード55の相互認証モジュール80と相互認証する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。

【0141】

ステップS142において、SAM62は、ICカードインタフェース64を介して、記憶モジュール81に記憶された、バックアップ鍵K i cで暗号化されている古いレシーバ51の記憶モジュール73のデータ（SAMのID番号、保存用鍵K s a v e、およびHDD52のIDを示すバックアップデータ）、およびEMDサービスセンタ1の公開鍵K p e s cで暗号化されているバックアップ鍵K i cを読み出す。ステップS143において、SAM62の相互認証モジュール71は、通信部61を介して、EMDサービスセンタ1の相互認証部17と相互認証する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS144において、SAM62は、通信部61を介して、バックアップ鍵K i cで暗号化されている記憶モジュール73のデータ、およびEMDサービスセンタ1の公開鍵K p e s cで暗号化されているバックアップ鍵K i cを、EMDサービスセンタ1のユーザ管理部18に送信する。

【0142】

ステップS145において、EMDサービスセンタ1のユーザ管理部18は、受信したバックアップ鍵K i cを自分自身の秘密鍵K s e s cで復号する。ステッ

ブ S 1 4 6 において、EMDサービスセンタ 1 のユーザ管理部 1 8 は、受信したバックアップデータを、バックアップ鍵 K i c で復号する。ステップ S 1 4 7 において、EMDサービスセンタ 1 のユーザ管理部 1 8 は、復号したバックアップデータを、相互認証部 1 7 から供給された一時鍵 K t e m p で、再度、暗号化する。ステップ S 1 4 8 において、EMDサービスセンタ 1 のユーザ管理部 1 8 は、一時鍵 K t e m p で暗号化されたバックアップデータを、レシーバ 5 1 の通信部 6 1 に送信する。

【0143】

ステップ S 1 4 9 において、レシーバ 5 1 の通信部 6 1 は、EMDサービスセンタ 1 のユーザ管理部 1 8 から受信したデータを、SAM 6 2 に送信し、SAM 6 2 は、そのデータを復号した後、記憶モジュール 7 3 に記憶させる。ステップ S 1 5 0 において、EMDサービスセンタ 1 のユーザ管理部 1 8 は、ICカード 5 5 にデータを記憶させた古い装置の SAM 6 2 の ID に対応するユーザ登録データベース（図 7）のデータを登録不可に設定し、処理を終了する。

【0144】

このように、新しいレシーバ 5 1 は、ICカード 5 5 のバックアップデータを読み込む。

【0145】

また、図 3 6 のステップ S 1 0 2 は、図 4 2 に示すフローチャートで説明される処理でもよい。ステップ S 1 6 1 乃至ステップ S 1 6 3 は、図 4 1 のステップ S 1 4 1 乃至ステップ S 1 4 3 とそれぞれ同様であるので、その説明は省略する。ステップ S 1 6 4 において、SAM 6 2 は、通信部 6 1 を介して、EMDサービスセンタ 1 の公開鍵 K p e s c で暗号化されているバックアップ鍵 K i c を、EMDサービスセンタ 1 のユーザ管理部 1 8 に送信する。

【0146】

ステップ S 1 6 5 において、EMDサービスセンタ 1 のユーザ管理部 1 8 は、受信したバックアップ鍵 K i c を自分自身の秘密鍵 K s e s c で復号する。ステップ S 1 6 6 において、EMDサービスセンタ 1 のユーザ管理部 1 8 は、復号したバックアップ鍵 K i c を、相互認証部 1 7 から供給された一時鍵 K t e m p で、再

度、暗号化する。ステップS167において、EMDサービスセンタ1のユーザ管理部18は、一時鍵Ktempで暗号化されたバックアップ鍵Kicを、レシーバ51の通信部61に送信し、バックアップ鍵Kicの復号のサービスに対するユーザへの課金の処理をする。

【0147】

ステップS168において、レシーバ51の通信部61は、EMDサービスセンタ1のユーザ管理部18から受信した一時鍵Ktempで暗号化されたバックアップ鍵Kicを、SAM62に送信し、SAM62は、一時鍵Ktempで暗号化されたバックアップ鍵Kicを復号する。ステップS169において、SAM62は、復号されたバックアップ鍵Kicで、ステップS162においてICカード55から読み出された古いレシーバ51の記憶モジュール73のデータ（SAMのID番号、保存用鍵Ksave、およびHDD52のIDを示すバックアップデータ）を復号し、記憶モジュール73に記憶させる。ステップS170において、EMDサービスセンタ1のユーザ管理部18は、ICカード55にデータを記憶させた古い装置のSAM62のIDに対応するユーザ登録データベース（図7）のデータを登録不可に設定し、処理を終了する。

【0148】

図42に示した読み込みの処理は、図41に示した処理に比較し、レシーバ51とEMDサービスセンタ1の送受信されるデータの量が少なくでき、従って、通信時間を短くできる。図41のステップS148において、図42のステップS167と同様に、EMDサービスセンタ1は、課金の処理を行ってもよい。

【0149】

図40に示す処理でバックアップされたデータを読み出す場合の処理を、図43に示すフローチャートを用いて説明する。ステップS181において、新しいレシーバ51のSAM62の相互認証モジュール71は、ICカード55の相互認証モジュール80と相互認証する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS182において、SAM62は、ICカードインタフェース64を介して、EMDサービスセンタ1の公開鍵Kpescで暗号化されている古いレシーバ51の記憶モジュール7

3 のデータ (SAM の ID 番号、保存用鍵 *K s a v e*、および HDD 5 2 の ID を示すバックアップデータ) を読み出す。

【0150】

ステップ S 1 8 3 において、SAM 6 2 の相互認証モジュール 7 1 は、通信部 6 1 を介して、EMD サービスセンタ 1 の相互認証部 1 7 と相互認証する。この認証処理は、図 3 3 乃至図 3 5 を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップ S 1 8 4 において、SAM 6 2 は、通信部 6 1 を介して、EMD サービスセンタ 1 の公開鍵 *K p e s c* で暗号化されている記憶モジュール 7 3 のデータを、EMD サービスセンタ 1 のユーザ管理部 1 8 に送信する。

【0151】

ステップ S 1 8 5 において、EMD サービスセンタ 1 のユーザ管理部 1 8 は、受信した記憶モジュール 7 3 のデータを自分自身の秘密鍵 *K s e s c* で復号する。ステップ S 1 8 6 において、EMD サービスセンタ 1 のユーザ管理部 1 8 は、復号したバックアップデータを、相互認証部 1 7 から供給された一時鍵 *K t e m p* で、再度、暗号化する。ステップ S 1 8 7 において、EMD サービスセンタ 1 のユーザ管理部 1 8 は、一時鍵 *K t e m p* で暗号化されたバックアップデータを、レシーバ 5 1 の通信部 6 1 に送信する。

【0152】

ステップ S 1 8 8 において、レシーバ 5 1 の通信部 6 1 は、EMD サービスセンタ 1 のユーザ管理部 1 8 から受信したデータを、SAM 6 2 に送信し、SAM 6 2 は、そのデータを復号した後、記憶モジュール 7 3 に記憶させる。ステップ S 1 8 9 において、EMD サービスセンタ 1 のユーザ管理部 1 8 は、IC カード 5 5 にデータを記憶させた古い装置の SAM 6 2 の ID に対応するユーザ登録データベース (図 7) のデータを登録不可に設定する。

【0153】

このように、図 4 0 に示す処理を用いたバックアップの場合、図 4 3 に示す処理により、新しいレシーバ 5 1 は、IC カード 5 5 のバックアップデータを読み込む。

【0154】

レシーバ 51 は、自分自身を登録する場合（図 30 のステップ S12 に対応する処理を実行する場合）、図 36 のフローチャートに示す処理を実行するが、レシーバ 51 に従属するレコーダ 53 を EMD サービスセンタ 1 に登録する場合、図 44 のフローチャートに示す処理を実行する。ステップ S201 において、レシーバ 51 の SAM62 は、記憶モジュール 73 に記憶された登録リストに、レコーダ 53 の ID を書き込む。ステップ S202 において、レシーバ 51 の相互認証モジュール 71 は、EMD サービスセンタ 1 の相互認証部 17 と相互認証する。この認証処理は、図 33 乃至図 35 を参照して説明した場合と同様であるので、ここでは説明を省略する。

【0155】

ステップ S203 において、EMD サービスセンタ 1 のユーザ管理部 18 は、レシーバ 51 の ID（図 37 に示す SAM62 の証明書に含まれる SAM62 の ID）を基に、ユーザ登録データベースを検索し、レシーバ 51 が登録不可であるか否かを判定し、レシーバ 51 が登録不可ではないと判定された場合、ステップ S204 に進み、レシーバ 51 の SAM62 は、記憶モジュール 73 に記憶している配送用鍵 Kd のバージョン、課金情報（後述の図 51 に示すフローチャートのステップ S357 の処理で記憶される）、および登録リスト、並びに HDD52 に記録された取扱方針を一時鍵 Ktemp で暗号化し、通信部 61 を介して送信する。ステップ S205 において、EMD サービスセンタ 1 のユーザ管理部 18 は、受信したデータを復号した後、課金情報を処理し、図 38 を参照して説明した、レシーバ 51 から受信した登録リストのレコーダ 53 に関する登録拒絶フラグ、およびステータスフラグなどのデータの部分を更新し、レシーバ 51 に対応するデータに応じた署名を付する。

【0156】

ステップ S206 において、EMD サービスセンタ 1 のユーザ管理部 18 は、レシーバ 51 が有する配送用鍵 Kd のバージョンが最新か否かを判定し、レシーバ 51 が有する配送用鍵 Kd のバージョンが最新であると判定された場合、ステップ S207 に進み、一時鍵 Ktemp で暗号化した、更新した登録リスト、および課金情報受信メッセージを、レシーバ 51 に送信し、レシーバ 51 は、更新し

た登録リスト、および課金情報受信メッセージを受信し、復号した後、記憶する。ステップ S 208 において、レシーバ 51 は、記憶モジュール 73 に記憶された課金情報を消去し、登録リストを、EMD サービスセンタ 1 のユーザ管理部 18 からステップ S 207 において受信したものに更新し、ステップ S 211 に進む。

【0157】

ステップ S 206 において、レシーバ 51 が有する配送用鍵 K d のバージョンが最新のものではないと判定された場合、ステップ S 209 に進み、EMD サービスセンタ 1 のユーザ管理部 18 は、一時鍵 K t e m p で暗号化した、最新バージョンの配送用鍵 K d、更新した登録リスト、および課金情報受信メッセージを、レシーバ 51 に送信し、レシーバ 51 は、最新バージョンの配送用鍵 K d、更新した登録リスト、および課金情報受信メッセージを受信し、復号した後、記憶する。ステップ S 210 において、レシーバ 51 は、記憶モジュール 73 に記憶された課金情報を消去し、登録リストを、EMD サービスセンタ 1 のユーザ管理部 18 からステップ S 209 において受信したものに更新し、配送用鍵 K d を最新バージョンのものに更新し、ステップ S 211 に進む。

【0158】

ステップ S 211 において、レシーバ 51 の SAM 62 は、更新した登録リストを参照し、レコーダ 53 が登録不可か否かを判定し、レコーダ 53 が登録不可でないと判定された場合、ステップ S 212 に進み、レシーバ 51 とレコーダ 53 は相互認証し、一時鍵 K t e m p を共有する。この認証処理は、図 33 乃至図 35 を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップ S 213 において、レコーダ 53 に、一時鍵 K t e m p で暗号化した、登録完了メッセージ、および配送用鍵 K d を送信し、レコーダ 53 は、登録完了メッセージ、および配送用鍵 K d を受信し、復号する。ステップ S 214 において、レコーダ 53 は、配送用鍵 K d を更新し、処理は終了する。

【0159】

ステップ S 203 において、レシーバ 51 が登録不可であると判定された場合、および、ステップ S 211 において、レコーダ 53 が登録不可であると判定さ

れた場合、処理は終了する。

【0160】

以上のように、レシーバ51に従属するレコーダ53は、レシーバ51を介して、EMDサービスセンタ1に登録される。

【0161】

図45は、図30のステップS13において、EMDサービスセンタ1がレシーバ51に送信した配送用鍵Kdを、レシーバ51が受け取る処理の詳細を説明するフローチャートである。ステップS221において、レシーバ51の相互認証モジュール71は、EMDサービスセンタ1の相互認証部17と相互認証する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS222において、レシーバ51のSAM62は、通信部61を介して、EMDサービスセンタ1のユーザ管理部18に証明書を送信し、EMDサービスセンタ1のユーザ管理部18は、証明書を受信する。ステップS223乃至ステップS230は、図44のステップS203乃至ステップS210と同様の処理であるのでその説明は省略する。

【0162】

このように、レシーバ51は、EMDサービスセンタ1のユーザ管理部18から配送用鍵Kdを受け取り、レシーバ51の課金情報をEMDサービスセンタ1のユーザ管理部18に送信する。

【0163】

次に、レシーバ51に従属するレコーダ53の配送用鍵Kdの受け取り処理（図38に示すステータスフラグが、レコーダ53の配送用鍵Kdの受け取りを許可する値を有する場合）を、図46に示すフローチャートを用いて説明する。ステップS241において、レシーバ51の相互認証モジュール71およびレコーダ53の図示せぬ相互認証モジュールは、相互認証する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。

【0164】

ステップS242において、レシーバ51は、レシーバ51の記憶モジュール

73に記憶する登録リストにレコーダ53のデータが載っているか否かを判定し、レシーバ51の記憶モジュール73に記憶する登録リストにレコーダ53のデータが載っていると判定された場合、ステップS243に進み、レシーバ51の記憶モジュール73に記憶する登録リストを基に、レコーダ53が登録不可であるか否かを判定する。ステップS243において、レコーダ53が登録不可ではないと判定された場合、ステップS244に進み、レコーダ53のSAM66は、レシーバ51のSAM62に、内蔵する記憶モジュールに記憶している配送用鍵Kd（後述する図46のステップS255でレシーバ51から受け取っている）のバージョンおよび課金情報（後述する図51に対応する処理のステップS357に相当する処理で記憶している）を一時鍵Ktempで暗号化して、送信し、レシーバ51のSAM62は、配送用鍵Kdのバージョンおよび課金情報を受信し、復号する。

【0165】

ステップS245において、レシーバ51の相互認証モジュール71は、通信部61を介して、EMDサービスセンタ1の相互認証部17と、相互認証する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS246において、EMDサービスセンタ1のユーザ管理部18は、レシーバ51のIDを基に、ユーザ登録データベースを検索し、レシーバ51が登録不可であるか否かを判定し、レシーバ51が登録不可ではないと判定された場合、ステップS247に進み、レシーバ51のSAM62は、通信部61を介して、EMDサービスセンタ1のユーザ管理部18に、一時鍵Ktempで暗号化した、記憶モジュール73に記憶している配送用鍵Kdのバージョン、課金情報、および登録リスト、HDD52に記録している取扱方針、並びにレコーダ53の課金情報を送信する。ステップS248において、EMDサービスセンタ1のユーザ管理部18は、受信したデータを復号した後、課金情報を処理し、図38で説明した、レシーバ51から受信した登録リストのレコーダ53に関する登録拒絶フラグ、ステータスフラグなどのデータの部分を更新し、レシーバ51に対応するデータに応じた署名を付する。

【0166】

ステップS 2 4 9乃至ステップS 2 5 4の処理は、図4 4に示すステップS 2 0 6乃至ステップS 2 1 1とそれぞれ同様であるので、その説明は省略する。

【0 1 6 7】

ステップS 2 5 4において、レシーバ5 1のSAM 6 2は、更新した登録リストを参照し、レコーダ5 3が登録不可か否かを判定し、レコーダ5 3が登録不可でないと判定された場合、ステップS 2 5 5に進み、レコーダ5 3に、一時鍵K t e m pで暗号化した、課金情報受信メッセージ、および配送用鍵K dを送信し、レコーダ5 3は、課金情報受信メッセージ、および配送用鍵K dを受信し、復号する。ステップS 2 5 6において、レコーダ5 3のSAM 6 6は、内蔵する記憶モジュールに記憶している、課金情報を消去し、配送用鍵K dを最新のバージョンに更新する。

【0 1 6 8】

ステップS 2 4 2において、レシーバ5 1の記憶モジュール7 3に記憶する登録リストにレコーダ5 3のデータが載っていないと判定された場合、ステップS 2 5 7に進み、図4 4に示したレコーダ5 3の登録処理を実行し、ステップS 2 4 4に進む。

【0 1 6 9】

ステップS 2 4 3において、レコーダ5 3が登録不可であると判定された場合、ステップS 2 4 6において、レシーバ5 1が登録不可であると判定された場合、および、ステップS 2 5 4において、レコーダ5 3が登録不可であると判定された場合、処理は終了する。

【0 1 7 0】

以上のように、レシーバ5 1に従属するレコーダ5 3は、レシーバ5 1を介して、配送用鍵K dを受け取る。

【0 1 7 1】

次に、図3 0のステップS 1 4に対応する、コンテンツプロバイダ2がサービスプロバイダ3にコンテンツプロバイダセキュアコンテナを送信する処理を、図4 7のフローチャートを用いて説明する。ステップS 2 7 1において、コンテンツプロバイダ2のウォーターマーク付加部3 2は、コンテンツサーバ3 1から読み

出したコンテンツに、コンテンツプロバイダ 2 を示す所定のウォーターマークを挿入し、圧縮部 3 3 に供給する。ステップ S 2 7 2 において、コンテンツプロバイダ 2 の圧縮部 3 3 は、ウォーターマークが挿入されたコンテンツを ATRAC2 等の所定の方式で圧縮し、暗号化部 3 4 に供給する。ステップ S 2 7 3 において、乱数発生部 3 5 は、コンテンツ鍵 K c o として用いる乱数を発生させ、暗号化部 3 4 に供給する。ステップ S 2 7 4 において、コンテンツプロバイダ 2 の暗号化部 3 4 は、DES などの所定の方式で、コンテンツ鍵 K c o を使用して、ウォーターマークが挿入され、圧縮されたコンテンツを暗号化する。

【 0 1 7 2 】

ステップ S 2 7 5 において、暗号化部 3 6 は、DES などの所定の方式で、図 3 0 のステップ S 1 1 の処理により、EMD サービスセンタ 1 から供給されている配送鍵 K d でコンテンツ鍵 K c o を暗号化する。ステップ S 2 7 6 において、コンテンツプロバイダ 2 のセキュアコンテナ作成部 3 8 は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 K c o、およびポリシー記憶部 3 7 から供給された取扱方針にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵 K s c p で暗号化し、図 1 3 に示すような署名を作成する。ステップ S 2 7 7 において、コンテンツプロバイダ 2 のセキュアコンテナ作成部 3 8 は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 K c o、ポリシー記憶部 3 7 から供給される取扱方針、およびステップ S 2 7 6 で生成した署名を含んだ、図 1 3 に示すようなコンテンツプロバイダセキュアコンテナを作成する。

【 0 1 7 3 】

ステップ S 2 7 8 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、サービスプロバイダ 3 の相互認証部 4 5 と相互認証する。この認証処理は、図 3 3 乃至図 3 5 を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップ S 2 7 9 において、コンテンツプロバイダ 2 のセキュアコンテナ作成部 3 8 は、サービスプロバイダ 3 に、コンテンツプロバイダセキュアコンテナに

、予め認証局から発行してもらった証明書を付して送信し、処理を終了する。

【 0 1 7 4 】

以上のように、コンテンツプロバイダ 2 は、サービスプロバイダ 3 に、コンテ

ンツプロバイダセキュアコンテナを送信する。

【0175】

コンテンツ鍵Kcoと共に取扱方針を配送用鍵Kdで暗号化する例の場合の、コンテンツプロバイダ2がサービスプロバイダ3にコンテンツプロバイダセキュアコンテナを送信する他の処理の詳細を、図48のフローチャートを用いて説明する。ステップS291乃至ステップS294の処理は、図47のステップS271乃至ステップS274の処理とそれぞれ同様であり、その説明は省略する。ステップS295において、コンテンツプロバイダ2の暗号化部36は、図31のステップS21の処理により、EMDサービスセンタ1から供給されている配送用鍵Kdを用いて、DESなどの所定の方式で、コンテンツ鍵Kcoおよびポリシー記憶部37から供給される取扱方針を暗号化する。

【0176】

ステップS296において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Kco、および暗号化された取扱方針にハッシュ関数を適用しハッシュ値を算出し、自分自身の秘密鍵Kscpで暗号化し、図25に示すような署名を作成する。ステップS297において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Kco、暗号化された取扱方針、および署名を含んだ、図25に示すようなコンテンツプロバイダセキュアコンテナを作成する。ステップS298およびステップS299の処理は、図47のステップS278およびステップS279の処理とそれぞれ同様であり、その説明は省略する。

【0177】

このように、コンテンツプロバイダ2は、サービスプロバイダ3に、暗号化された取扱方針を含むコンテンツプロバイダセキュアコンテナを送信する。

【0178】

次に、図30のステップS15に対応する、サービスプロバイダ3がレシーバ51にサービスプロバイダセキュアコンテナを送信する処理の詳細を図49のフローチャートを用いて説明する。ステップS311において、サービスプロバイ

ダ3の値付け部42は、コンテンツプロバイダ2のセキュアコンテナ作成部38から送信されたコンテンツプロバイダセキュアコンテナに付された証明書に含まれる署名を確認し、証明書の改竄がなければ、コンテンツプロバイダ2の公開鍵 $K_{p\ c\ p}$ を取り出す。証明書の署名の確認は、図35のステップS83における処理と同様であるので、その説明は省略する。

【0179】

ステップS312において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダ2のセキュアコンテナ作成部38から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ2の公開鍵 $K_{p\ c\ p}$ で復号し、得られたハッシュ値が、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 $K_{c\ o}$ 、および取扱方針にハッシュ関数を適用し得られたハッシュ値と一致することを確認し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。改竄が発見された場合は、処理を終了する。

【0180】

コンテンツプロバイダセキュアコンテナに改竄がない場合、ステップS313において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダセキュアコンテナから取扱方針を取り出す。ステップS314において、サービスプロバイダ3の値付け部42は、取扱方針を基に、図17で説明した価格情報を作成する。ステップS315において、サービスプロバイダ3のセキュアコンテナ作成部44は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 $K_{c\ o}$ 、取扱方針、価格情報、並びに暗号化されたコンテンツ、暗号化されたコンテンツ鍵 $K_{c\ o}$ 、取扱方針、コンテンツプロバイダ2により生成された署名、および価格情報にハッシュ関数を適用して得られたハッシュ値を、自分自身の秘密鍵 $K_{s\ s\ p}$ で暗号化し、得られた値を署名として図15に示すようなサービスプロバイダセキュアコンテナを作成する。

【0181】

ステップS316において、サービスプロバイダ3の相互認証部45は、レシーバ51の相互認証モジュール71と相互認証する。この認証処理は、図33乃至図35を参照して説明した場合と同様であるので、ここでは説明を省略する。

ステップS 3 1 7において、サービスプロバイダ3のセキュアコンテナ作成部44は、レシーバ51の通信部61に、証明書を付したサービスプロバイダセキュアコンテナを送信し、処理を終了する。

【0182】

このように、サービスプロバイダ3は、レシーバ51にサービスプロバイダセキュアコンテナを送信する。

【0183】

コンテンツプロバイダ2において、取扱方針が配送用鍵K dで暗号化され、かつ、サービスプロバイダ3が取扱制御情報を作成する例の場合の、サービスプロバイダ3がレシーバ51にサービスプロバイダセキュアコンテナを送信する処理の詳細を、図50のフローチャートを用いて説明する。ステップS 3 3 1およびステップS 3 3 2の処理は、図49のステップS 3 1 1およびステップS 3 1 2の処理とそれぞれ同様であるので、その説明は省略する。ステップS 3 3 3において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダセキュアコンテナに含まれる暗号化された取扱方針を復号する。ステップS 3 3 4において、サービスプロバイダ3の値付け部42は、取扱方針を基に、図23で説明した取扱制御情報を作成する。ステップS 3 3 5乃至ステップS 3 3 8の処理は、図49のステップS 3 1 4およびステップS 3 1 7の処理とそれぞれ同様であるので、その説明は省略する。

【0184】

このように、サービスプロバイダ3は、レシーバ51に暗号化された取扱方針を含むサービスプロバイダセキュアコンテナを送信する。

【0185】

図30のステップS 1 6に対応する、適正なサービスプロバイダセキュアコンテナを受信した後の、レシーバ51の課金処理の詳細を、図51のフローチャートを用いて説明する。ステップS 3 5 1において、レシーバ51の復号/暗号化モジュール74は、配送用鍵K dでコンテンツ鍵K c oを復号できるか否かを判定し、配送用鍵K dでコンテンツ鍵K c oを復号できないと判定された場合、ステップS 3 5 2で、レシーバ51は、図45で説明した配送用鍵K dの受け取り

処理を実行し、ステップS353に進む。ステップS351において、配送用鍵Kdでコンテンツ鍵Kcoを復号できると判定された場合、手続は、ステップS352をスキップし、ステップS353に進む。ステップS353において、レシーバ51の復号ユニット91は、図30のステップS13の処理により、記憶モジュール73に記憶されている配送用鍵Kdで、コンテンツ鍵Kcoを復号する。

【0186】

ステップS354において、レシーバ51の課金処理モジュール72は、サービスプロバイダセキュアコンテナに含まれる取扱方針および価格情報を取り出し、図19および図20で説明した課金情報および使用許諾条件情報を生成する。ステップS355において、レシーバ51の課金処理モジュール72は、記憶モジュール73に記憶している課金情報およびステップS354で算出された課金情報から、現在の課金が課金の上限以上であるか否かを判定し、現在の課金が課金の上限以上であると判定された場合、ステップS356に進み、レシーバ51は図45で説明した配送用鍵Kdの受け取り処理を実行し、新たな配送用鍵Kdを受け取り、ステップS357に進む。ステップS355において、現在の課金が課金の上限未満であると判定された場合、ステップS356はスキップされ、ステップS357に進む。

【0187】

ステップS357において、レシーバ51の課金処理モジュール72は、記憶モジュール73に課金情報を記憶させる。ステップS358において、レシーバ51の課金処理モジュール72は、ステップS354にて生成した使用許諾条件情報をHDD52に記録する。ステップS359において、レシーバ51のSAM62は、HDD52にサービスプロバイダセキュアコンテナから取り出した取扱方針を記録させる。

【0188】

ステップS360において、レシーバ51の復号／暗号化モジュール74は、使用許諾条件情報の全体にハッシュ関数を適用しハッシュ値を算出する。ステップS361において、レシーバ51の記憶モジュール73は、使用許諾条件情報

のハッシュ値を記憶する。

【0189】

ステップS362において、レシーバ51の暗号化ユニット93は、コンテンツ鍵Kcoを保存用鍵Ksaveで暗号化する。ステップS363において、レシーバ51のSAM62は、暗号化されたコンテンツ鍵KcoをHDD52に記憶させる。

【0190】

以上のように、レシーバ51は、課金情報を記憶モジュール73に記憶すると共に、コンテンツ鍵Kcoを配送用鍵Kdで復号し、再度、コンテンツ鍵Kcoを保存用鍵Ksaveで暗号化し、HDD52に記録させる。保存用鍵Ksaveは、記憶モジュール73に記憶されている。

【0191】

レコーダ53も、同様の処理で、課金情報をSAM66内の記憶モジュールに記憶すると共に、コンテンツ鍵Kcoを配送用鍵Kdで復号し、再度、コンテンツ鍵Kcoを保存用鍵Ksaveで暗号化し、HDD52に記録させる。保存用鍵Ksaveは、SAM66内の記憶モジュールに記憶されている。なお、レシーバ51とレシーバ53においてそれぞれ保持される保存用鍵Ksaveは、通常、違う鍵データとされている。

【0192】

図30のステップS17に対応するレシーバ51がコンテンツを再生する処理の詳細を、図52のフローチャートを用いて説明する。ステップS381において、レシーバ51の復号/暗号化モジュール74は、HDD52から、図51のステップS358で記憶した使用許諾条件情報およびステップS363で記憶した暗号化されたコンテンツ鍵Kcoを読み出す。ステップS382において、レシーバ51の復号/暗号化モジュール74は、使用許諾条件情報の全体にハッシュ関数を適用しハッシュ値を算出する。

【0193】

ステップS383において、レシーバ51の復号/暗号化モジュール74は、ステップS382において算出されたハッシュ値が、図51のステップS360

で記憶モジュール 73 に記憶されたハッシュ値と一致するか否かを判定し、ステップ S382 において算出されたハッシュ値が、記憶モジュール 73 に記憶されたハッシュ値と一致すると判定された場合、ステップ S384 に進み、使用回数の値などの使用許諾条件情報に含まれる所定の情報を更新する。ステップ S385 において、レシーバ 51 の復号／暗号化モジュール 74 は、更新した使用許諾条件情報の全体にハッシュ関数を適用しハッシュ値を算出する。ステップ S386 において、レシーバ 51 の記憶モジュール 73 は、ステップ S385 で算出した使用許諾条件情報のハッシュ値を記憶する。ステップ S387 において、レシーバ 51 の復号／暗号化モジュール 74 は、HDD 52 に更新した使用許諾条件情報を記録させる。

【0194】

ステップ S388 において、SAM 62 の相互認証モジュール 71 と伸張部 63 の相互認証モジュール 75 は、相互認証し、SAM 62 および伸張部 63 は、一時鍵 K_{temp} を記憶する。この認証処理は、図 33 乃至図 35 を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数 $R1$ 、 $R2$ 、 $R3$ 、またはその組み合わせが、一時鍵 K_{temp} として用いられる。ステップ S389 において、復号／暗号化モジュール 74 の復号ユニット 91 は、図 51 のステップ S363 にて HDD 52 に記録されたコンテンツ鍵 K_{co} を、記憶モジュール 73 に記憶された保存用鍵 K_{save} で復号する。ステップ S390 において、復号／暗号化モジュール 74 の暗号化ユニット 93 は、復号されたコンテンツ鍵 K_{co} を一時鍵 K_{temp} で暗号化する。ステップ S391 において、SAM 62 は、一時鍵 K_{temp} で暗号化されたコンテンツ鍵 K_{co} を伸張部 63 に送信する。

【0195】

ステップ S392 において、伸張部 63 の復号モジュール 76 は、コンテンツ鍵 K_{co} を一時鍵 K_{temp} で復号する。ステップ S393 において、SAM 62 は、HDD 52 に記録されたコンテンツを読み出し、伸張部 63 に送信する。ステップ S394 において、伸張部 63 の復号モジュール 77 は、コンテンツをコンテンツ鍵 K_{co} で復号する。ステップ S395 において、伸張部 63 の伸張モジ

ルール 78 は、復号されたコンテンツを ATRAC2 などの所定の方式で伸張する。ステップ S396 において、伸張部 63 のウォータマーク付加モジュール 79 は、伸張されたコンテンツにレシーバ 51 を特定する所定のウォータマークを挿入する。ステップ S397 において、レシーバ 51 は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

【0196】

ステップ S383 において、ステップ S382 において算出されたハッシュ値が、記憶モジュール 73 に記憶されたハッシュ値と一致しないと判定された場合、ステップ S398 において、SAM62 は、図示せぬ表示装置にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

【0197】

このように、レシーバ 51 は、コンテンツを再生する。

【0198】

図 53 は、図 11 の構成を有するユーザホームネットワーク 5 において、レシーバ 51 がデコーダ 56 にコンテンツを再生させる処理を説明するフローチャートである。ステップ S411 乃至ステップ S417 の処理は、図 52 のステップ S381 乃至ステップ S387 の処理とそれぞれ同様であるので、その説明は省略する。

【0199】

ステップ S418 において、SAM62 の相互認証モジュール 71 とデコーダ 56 の相互認証モジュール 101 は、相互認証し、一時鍵 K_{temp} が共有される。この認証処理は、図 33 乃至図 35 を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数 $R1$ 、 $R2$ 、 $R3$ 、またはその組み合わせが、一時鍵 K_{temp} として用いられる。ステップ S419 において、復号／暗号化モジュール 74 の復号ユニット 91 は、HDD52 に記録されたコンテンツ鍵 K_c を、記憶モジュール 73 に記憶された保存用鍵 K_{save} で復号する。ステップ S420 において、復号／暗号化モジュール 74 の暗号化ユニット 93 は、復号されたコンテンツ鍵 K_c を一時鍵 K_{temp} で暗号化する。ステップ S421 において、SAM62 は、一時鍵 K_{temp} で暗号化され

たコンテンツ鍵K c oをデコーダ56に送信する。

【0200】

ステップS422において、デコーダ56の復号モジュール102は、コンテンツ鍵K c oを一時鍵K t e m pで復号する。ステップS423において、SAM62は、HDD52に記録されたコンテンツを読み出し、デコーダ56に送信する。ステップS424において、デコーダ56の復号モジュール103は、コンテンツをコンテンツ鍵K c oで復号する。ステップS425において、デコーダ56の伸張モジュール104は、復号されたコンテンツをATRAC2などの所定の方式で伸張する。ステップS426において、デコーダ56のウォーターマーク付加モジュール105は、伸張されたコンテンツにデコーダ56を特定する所定のウォーターマークを挿入する。ステップS427において、デコーダ56は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

【0201】

ステップS428の処理は、図52のステップS398の処理と同様であるので、その説明は省略する。

【0202】

以上のように、ユーザホームネットワークが図11に示す構成を有する場合、レシーバ51が受信したコンテンツは、デコーダ56で再生される。

【0203】

なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動画像データ、静止画像データ、文書データ、またはプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であればMPEG(Moving Picture Experts Group)などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

【0204】

また、共通鍵暗号は、ブロック暗号であるDESを使用して説明したが、NTT(商標)が提案するFEAL、IDEA(International Data Encryption Algorithm)、または1ビット乃至数ビット単位で暗号化するストリーム暗号などでもよい。

【0205】

さらに、コンテンツおよびコンテンツ鍵Kcoの暗号化は、共通鍵暗号方式を利用するとして説明したが、公開鍵暗号方式でもよい。

【0206】

図54は、本発明を適用したEMDシステムの他の構成例を表している。なお、図中、図1および図10における場合と対応する部分については、同一の符号を付してある。すなわち、この例においては、ユーザホームネットワーク5に代えて、ユーザホームネットワーク200が設けられ、そのユーザホームネットワーク200には、レコーダ53に代えて、レシーバ201およびレシーバ202が、レシーバ51に従属（接続）されている。

【0207】

レシーバ201は、レシーバ51と同様の構成を有しており、レシーバ51のSAM62および記憶モジュール73のそれぞれに対応するSAM210および記憶モジュール211等を有し、そしてHDD203に接続されている。レシーバ202も、レシーバ51と同様の構成を有しており、SAM220および記憶モジュール221等を有している。レシーバ202は、レシーバ201にも接続（従属）する。ただし、レシーバ202は、HDDのような記録媒体には接続されていない。

【0208】

レシーバ51は、図10に示す構成を有するが、この例において、SAM62の記憶モジュール73には、図38で示した登録リストに代えて、図55に示すような登録リストが記憶されている。この登録リストは、表形式に情報が記憶されているリスト部、および登録リストを保持する機器についての所定の情報が記憶されている対象SAM情報部より構成されている。

【0209】

対象SAM情報部には、この登録リストを保有する機器のSAMID、この例の場合、レシーバ51のSAM62のIDが（「対象SAMID」の欄に）記憶されている。対象SAM情報部にはまた、この登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ51には、レシーバ201およびレシーバ202の2機の機器が接続されているので

、自分自身を含む合計値3が（「接続されている機器数」の欄に）記憶されている。

【0210】

リスト部は、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、「状態情報」、「登録条件署名」、および「登録リスト署名」の9個の項目から構成され、この例の場合、レシーバ51の登録条件、レシーバ201の登録条件、およびレシーバ202の登録条件として、それぞれの項目に所定の情報が記憶されている。

【0211】

「SAMID」には、機器のSAMのIDが記憶される。この例の場合、レシーバ51のSAM62のID、レシーバ201のSAM210のID、およびレシーバ202のSAM220のIDが記憶されている。「ユーザID」には、対応する機器（レシーバ51、レシーバ201、およびレシーバ202）のユーザのユーザIDが記憶される。

【0212】

「購入処理」には、対応する機器が、コンテンツを購入（具体的には、使用許諾条件やコンテンツ鍵Kcoを購入）するための処理を行うことができるか否かを示す情報（“可”または“不可”）が記憶される。この例の場合、レシーバ51およびレシーバ201は、コンテンツを購入するための処理を行うことができるので、それぞれに対応する「購入処理」には、“可”が記憶されている。レシーバ202は、購入したコンテンツを記録する、例えば、HDDのような記録媒体に接続されていないので、コンテンツを購入する処理を行うことができず、そのため、レシーバ202に対応する「購入処理」には、“不可”が記憶されている。

【0213】

「課金処理」には、対応する機器が、EMDサービスセンタ1との間で、課金処理を行うことができるか否かを示す情報（“可”または“不可”）が記憶される。なお、課金処理が行えるか否かは、EMDサービスセンタ1において、機器をEMDシステム登録する際に決定される。この例の場合、レシーバ51は、レシーバ51課金処理を行うことができる機器として登録されているので、対応する「課金処

理」には、「可」が記憶されている。一方、レシーバ201およびレシーバ202は、この例の場合、課金処理を行うことができない機器として登録されているので、レシーバ201およびレシーバ202のそれぞれに対応する「課金処理」には、「不可」が記憶されている。なお、レシーバ202においては、コンテンツの購入がなされないので、課金は計上されず、課金自体の必要がない。

【0214】

「課金機器」には、対応する機器において計上された課金に対する課金処理を行う機器のSAMのIDが記憶される。この例の場合、レシーバ51（SAM62）は、自分自身の課金に対する課金処理を行うことができるので、その対応する「課金機器」には、レシーバ51のSAM62のIDが記憶されている。レシーバ51はまた、課金処理を行うことができないレシーバ201に代わり、レシーバ201により計上される課金に対する課金処理を行うので、レシーバ201に対応する「課金機器」には、レシーバ51のSAM62のIDが記憶されている。レシーバ202においては、上述したように、コンテンツが購入されず、課金も計上されないため、レシーバ202に対する課金処理は必要とされない。そのため、レシーバ202に対応する「課金機器」には、課金処理を行う機器が存在しないことを示す情報（「なし」）が記憶されている。

【0215】

「コンテンツ供給機器」には、対応する機器が、コンテンツの供給をサービスプロバイダ3からではなく、接続される他の機器から受ける場合、コンテンツを供給することができる機器のSAMのIDが記憶される。この例の場合、レシーバ51およびレシーバ201は、コンテンツの供給をサービスプロバイダ3から受けるため、それぞれに対応する「コンテンツ供給機器」には、コンテンツを供給する機器が存在しない旨を示す情報（「なし」）が記憶されている。レシーバ202は、ネットワーク4に接続されていないことから、コンテンツの供給をサービスプロバイダ3から受けることができず、レシーバ51またはレシーバ201からコンテンツの供給を受ける。そのため、レシーバ202に対応する「コンテンツ供給機器」には、レシーバ51のSAM62のIDおよびレシーバ201のSAM210のIDが記憶されている。

【0216】

「状態情報」には、対応する機器の動作制限条件が記憶される。何ら制限されていない場合は、その旨を示す情報（”制限なし”）、一定の制限が課せられている場合は、その旨を示す情報（”制限あり”）、また動作が停止される場合には、その旨を示す情報（”停止”）が記憶される。例えば、課金処理が成功しなかった場合、その機器に対応する「状態情報」には、”制限あり”が設定される（詳細は後述する）。この例の場合、「状態情報」に”制限あり”が設定された機器においては、すでに購入されたコンテンツの再生（解読）処理は実行されるが、新たなコンテンツを購入するための処理は実行されなくなる。すなわち、一定の制限が機器に課せられる。また、コンテンツの不正複製などの違反行為が発覚した場合、「状態情報」には、”停止”が設定され、機器の動作が停止される。これにより、その機器はEMDシステムからのサービスを、一切受けうることができなくなる。

【0217】

この例の場合、レシーバ51、レシーバ201、およびレシーバ202に対して、何ら制限が課せられていないものとし、それぞれに対応する「状態情報」には、”なし”が設定されている。

【0218】

「登録条件署名」には、上述したように、各機器（レシーバ51、レシーバ201、およびレシーバ202）の登録条件として、それぞれ、「SAMID」、「購入処理」、「課金処理」、「課金代行機器」、「コンテンツ供給機器」、「状態情報」、および「公開鍵」に記憶されている情報に対するEMDサービスセンタ1による署名が記憶されている。

【0219】

「登録リスト署名」には、登録リストに設定されている全てのデータに対する、EMDサービスセンタ1の署名が記憶されている。

【0220】

図56は、レシーバ201のSAM210の記憶モジュール211に記憶されている、レシーバ201の登録リストを表している。この登録リストの対象SAM情

報部には、レシーバ201のSAM210のID、その登録リストの有効期限、バージョン番号、接続されている機器の数（この例では、レシーバ201には、レシーバ51およびレシーバ202の2機が接続され、自分自身を含めた合計数3）が記憶されている。リスト部には、図55のレシーバ51の登録リストのリスト部と同様の情報が記憶されている。

【0221】

図57は、レシーバ202のSAM220の記憶モジュール221に記憶されている、レシーバ202の登録リストを表している。この登録リストの対象SAM情報部には、レシーバ202のSAM220のID、その登録リストの有効期限、バージョン番号、接続されている機器の数（この例では、レシーバ202には、レシーバ51およびレシーバ201の2機が接続され、自分自身を含めた合計数3）が記憶されている。リスト部には、この例の場合、図55および図56の登録リストのリスト部に登録されているレシーバ51、レシーバ201、およびレシーバ202の登録条件のうち、レシーバ202の登録条件のみが記憶されている。

【0222】

次に、図55、図56、および図57に示したそれぞれの登録リストを、レシーバ51の記憶モジュール73、レシーバ201の記憶モジュール211、およびレシーバ202の記憶モジュール221に記憶させるための処理手順を、図58のフローチャートを参照して説明する。

【0223】

ステップS501において、レシーバ51の登録処理が実行される。ステップS501における登録処理の詳細は、図59のフローチャートに示されている。

【0224】

ステップS601乃至S608においては、図36のステップS101乃至S108における場合と同様の処理が実行されるので、その説明は省略するが、ステップS608において、EMDサービスセンタ1のユーザ管理部18は、ユーザ登録データベースに基づいて、図60に示すような登録リストを作成する。ここで作成された登録リストは、図55に示した登録リストにおいて、レシーバ51の登録条件のみが登録されているものに相当する。

【0225】

ステップS609乃至S614においては、図36のステップS109乃至S114における場合と同様の処理が実行されているので、その詳細の説明は省略するが、ステップS612において、レシーバ51のSAM62は、ステップS611で、EMDサービスセンタ1から送信された登録リストを、一時鍵Ktempで復号し、記憶モジュール73に記憶させる。このように、図60に示した登録リストが、レシーバ51の記憶モジュール73に記憶されたとき、処理は終了し、図58のステップS502に進む。

【0226】

ステップS502において、レシーバ201およびレシーバ202の登録処理が実行される。ステップS502における登録処理の詳細は、図61のフローチャートに示されている。

【0227】

ステップS701において、レシーバ51のSAM62は、HDD52に記憶されている登録リスト（図60）に、図62に示すように、レシーバ201のSAM210のIDおよびレシーバ202のSAM220のIDを「SAMID」に書き加え、そしてそれらに対応して、所定の情報を、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」の各項目に書き込む。

【0228】

この例の場合、レシーバ201のSAM210のIDが設定された「SAMID」に対応して、「購入処理」に”可”が、「課金処理」に”不可”が、「課金機器」にレシーバ51のSAM62のIDが、そして「コンテンツ供給機器」に”なし”が書き込まれる。またレシーバ202のSAM220のIDが設定された「SAMID」に対応して、「購入処理」に”不可”が、「課金処理」に”不可”が、「課金機器」に”なし”が、そして「コンテンツ供給機器」にレシーバ51のSAM62のIDおよびレシーバ201のSAM210のIDが書き込まれる。なお、ここで、「購入処理」

、「課金処理」、「課金機器」、および「コンテンツ供給機器」のそれぞれに書き込まれる情報は、例えば、レシーバ201およびレシーバ202が、レシーバ51に接続される際に設定された条件により決定される。

【0229】

次に、ステップS702において、レシーバ51とEMDサービスセンタ1との相互認証が行われる。この相互認証は、図33乃至図35を参照して説明した場合と同様の処理であるので、その説明は省略する。

【0230】

ステップS703において、レシーバ51のSAM62は、HDD52に記憶されている、課金情報に関連した取扱方針を一時鍵Ktempで暗号化し、ステップS701で新たな情報が書き加えられた登録リスト、記憶モジュール73に記憶されている配送用鍵Kdのバージョン、および課金情報とともに、EMDサービスセンタ1に送信する。

【0231】

ステップS704において、EMDサービスセンタ1のユーザ管理部18は、ステップS703で、レシーバ51から送信されてきた情報を受信し、復号する。その後、EMDサービスセンタ1のユーザ管理部18が、登録リストの「状態情報」に”停止”を設定すべき不正行為がレシーバ201およびレシーバ202において存在するか否かを確認する。

【0232】

次に、ステップS705において、EMDサービスセンタ1のユーザ管理部18は、ユーザ登録データベースと、ステップS704でのユーザ管理部18による確認結果に基づいて、レシーバ201およびレシーバ202の登録条件を登録リストのリスト部に設定し、それに署名を付して、レシーバ51の登録リスト（図55）、を作成し、そのリスト部の情報を記憶する。

【0233】

次に、ステップS706において、EMDサービスセンタ1のユーザ管理部18は、ステップS705で作成された登録リスト（レシーバ51の登録リスト）を、一時鍵Ktempで暗号化して、レシーバ51に送信する。

【0234】

ステップS707において、レシーバ51のSAM62は、ステップS706で、EMDサービスセンタ1から送信された登録リストを受信し、復号した後、記憶

モジュール 73 に記憶させる。これにより、ステップ S 706 で送信されてきたレシーバ 51 の登録リスト（図 55）が、ステップ S 612（図 59）で記憶された図 60 に示した登録リストに代えて、記憶モジュール 73 に記憶される。これにより、処理は終了され、図 58 のステップ S 503 に進む。

【0235】

ステップ 503 において、レシーバ 51 とレシーバ 201 の相互認証が行われるが、この相互認証処理は、図 33 乃至図 35 を参照して説明した場合と同様の処理であるので、その説明は省略する。

【0236】

次に、ステップ S 504 において、レシーバ 51 の SAM 62 は、ステップ S 707 で記憶モジュール 73 に記憶された登録リストから、レシーバ 201 の登録リスト（図 56）を生成してレシーバ 201 に送信する。

【0237】

ステップ S 505 において、レシーバ 201 の SAM 210 は、ステップ S 504 でレシーバ 51 から送信された登録リストを受信し、復号した後、記憶モジュール 211 に記憶させる。これにより、図 56 に示した登録リストが、記憶モジュール 211 に記憶される。

【0238】

次に、ステップ 506 において、レシーバ 51 とレシーバ 202 の相互認証が行われるが、この相互認証処理は、図 33 乃至図 35 を参照して説明した場合と同様の処理であるので、その説明は省略する。

【0239】

ステップ S 507 において、レシーバ 51 の SAM 62 は、ステップ S 707 で記憶モジュール 73 に記憶された登録リストのうち、レシーバ 202 の登録リスト（レシーバ 202 の登録条件のみが記憶されている登録リスト（図 57））を、レシーバ 202 に送信する。

【0240】

次に、ステップ S 508 において、レシーバ 202 の SAM 220 は、ステップ S 507 でレシーバ 51 から送信された登録リストを受信し、復号した後、記憶

モジュール 221 に記憶させる。これにより、図 57 に示した登録リストが、記憶モジュール 221 に記憶される。その後、処理は終了される。

【0241】

以上のようにして、レシーバ 51、レシーバ 201、およびレシーバ 202 は、それぞれの登録リストを取得し、それを保持する。

【0242】

次に、上述したように作成され、各レシーバに保持された登録リストの利用方法を、図 51 のフローチャートで説明した課金処理に対応させて説明する。

【0243】

図 51 のフローチャートで説明された課金処理において、ステップ S355 で、現在の課金の合計が、予め設定された上限額以上であると判定された場合、ステップ S356 に進み、配送用鍵 Kd の受け取り処理が実行される。この例の場合、図 45 のフローチャートで説明された手順に代わり、図 63 のフローチャートに示されている手順に従って処理が実行される。

【0244】

すなわち、ステップ S801 において、レシーバ 51 と EMD サービスセンタ 1 との相互認証が行われる。この相互認証は、図 33 乃至図 35 を参照して説明した場合と同様の処理であるので、その説明は省略する。

【0245】

次に、ステップ S802 において、レシーバ 51 の SAM62 は、必要に応じて、EMD サービスセンタ 1 のユーザ管理部 18 に証明書を送信する。ステップ S803 において、レシーバ 51 の SAM62 は、HDD52 に記憶されている、課金に関連する取扱方針を一時鍵 Ktemp で暗号化して、記憶モジュール 73 に記憶されている配送用鍵 Kd のバージョン、課金情報、および登録リストとともに、EMD サービスセンタ 1 に送信する。

【0246】

ステップ S804 において、EMD サービスセンタ 1 のユーザ管理部 18 は、ステップ S803 で、レシーバ 51 から送信された情報を受信し、復号した後、EMD サービスセンタ 1 の監査部 21 が、登録リストの「状態情報」に”停止”が設

定されるべき不正行為がレシーバ51、レシーバ201、およびレシーバ202において存在するか否かを確認する。

【0247】

次に、ステップS805において、EMDサービスセンタ1のユーザ管理部18は、ステップS804での確認結果に基づいて、レシーバ51に不正行為が存在するか否かを判定し、レシーバ51に不正行為が存在しないと判定した場合、ステップS806に進む。

【0248】

ステップS806において、EMDサービスセンタ1の課金請求部19は、ステップS803で受信された課金情報を解析し、ユーザの支払い金額を算出する処理等を行う。次に、ステップS807において、EMDサービスセンタ1のユーザ管理部18は、ステップS806における処理により、決済が成功したか否かを確認し、その確認結果に基づいて、返却メッセージを作成する。この場合、レシーバ51およびレシーバ201の両者の課金に対する決済が共に成功したとき（全ての機器に対する決済が成功したとき）、成功返却メッセージが作成される。また、レシーバ51またはレシーバ201のいずれか一方の課金に対する決済が成功しなかったとき、またはレシーバ51およびレシーバ201の両者の課金に対する決済が成功しなかったとき（全ての機器に対する決済が成功しなかったとき）、失敗返却メッセージが作成される。

【0249】

次に、ステップS808において、EMDサービスセンタ1のユーザ管理部18は、ユーザ登録データベース、ステップS804における不正行為が存在するか否かの確認結果、およびステップS807における決済が成功したか否かの確認結果に基づいて、レシーバ51、レシーバ201、およびレシーバ202の登録条件を設定し、それに署名を付して、登録リストをそれぞれ作成する。

【0250】

例えば、ステップS804で、レシーバ201またはレシーバ202において不正行為が確認された場合、それらに対応する「状態情報」には”停止”が設定され、この場合、今後、全ての処理が停止される。すなわち、EMDシステムから

のサービスを一切受けることができなくなる。また、ステップS807で、決済が成功しなかったと確認された場合、「状態情報」には”制限あり”が設定され、この場合、すでに購入したコンテンツを再生する処理は可能とされるが、新たにコンテンツを購入する処理は実行できなくなる。

【0251】

次に、ステップS809に進み、EMDサービスセンタ1のユーザ管理部18は、一時鍵Ktempで、最新バージョンの配送用鍵Kd（図3で示した3月分の最新バージョンの配送用鍵Kd）およびステップS808で作成された登録リストを暗号化し、ステップS807で作成された返却メッセージとともにレシーバ51に送信する。

【0252】

ステップS810において、レシーバ51のSAM62は、ステップS809でEMDサービスセンタ1から送信された情報を受信し、復号した後、記憶モジュール73に記憶させる。このとき、記憶モジュール73に記憶されていた課金情報は消去され、自分の登録リストおよび配送用鍵Kdは更新される。

【0253】

次に、ステップS811において、レシーバ51のSAM62は、ステップS810で受信した返却メッセージが、成功返却メッセージであったかまたは失敗返却メッセージであったかを判定し、成功返却メッセージであったと判定した場合、ステップS812に進む。

【0254】

ステップS812において、レシーバ51のSAM62は、レシーバ201およびレシーバ202に対して、それぞれ相互認証処理（図33乃至図35を参照して説明した処理）を行った後、レシーバ201およびレシーバ202のそれぞれに、それぞれの登録リストと、配送用鍵Kdを送信する。

【0255】

ステップS811において、ステップS810で受信した返却メッセージが、失敗返却メッセージであったと判定した場合、レシーバ51のSAM62は、ステップS813に進み、ステップS801で記憶モジュール73に記憶させた登録

リスト（更新された登録リスト）を参照し、“制限あり”が「状態情報」に設定されているレシーバ（この例の場合、レシーバ51の自分自身、またはレシーバ201）を検出する。

【0256】

次に、ステップS814において、レシーバ51のSAM62は、ステップS810で検出したレシーバに対して、所定の処理（REVOKE処理）を実行し、そのレシーバにおいて実行される処理を制限する。すなわち、この場合、新たにコンテンツを購入するための処理が実行できないようにする。

【0257】

ステップS805において、レシーバ51において不正行為が確認された場合、ステップS815に進み、EMDサービスセンタ1は、レシーバ51、レシーバ201、およびレシーバ202に対応する「状態情報」の全てに“停止”を設定し、登録リストを作成し、ステップS816において、レシーバ51に送信する。なお、図36のフローチャートで示した登録処理を、レシーバ201またはレシーバ202に対して行うことより、レシーバ201またはレシーバ202におけるコンテンツの利用が可能となる。

【0258】

次に、ステップS817において、レシーバ51は、ステップS816でEMDサービスセンタ1から送信された登録リストを受信し、登録リストを更新する。すなわち、この場合、配送用鍵Kdは、レシーバ51、レシーバ201、およびレシーバ202には、供給されず、レシーバ51、レシーバ201、およびレシーバ202は、供給されるコンテンツを再生することができなくなり、その結果、EMDシステムにおけるサービスを一切受けることができなくなる。

【0259】

ステップS812において、レシーバ201およびレシーバ202に登録リストおよび配送用鍵Kdが送信されたとき、ステップS814において、「状態情報」に“制限あり”が設定されたレシーバに対してREVOKE処理が実行されたとき、またはステップS817において、「状態情報」に“停止”が設定された登録リストに更新されたとき、処理は終了され、図51のステップS357に進む。

【0260】

ステップ S 3 5 7 乃至 S 3 6 5 における処理は、すでに説明されているので、ここでの説明は省略する。

【0261】

以上のように、登録リストが EMD サービスセンタ 1 に送信されると（図 6 3 のステップ S 8 0 3）、EMD サービスセンタ 1 において、レシーバの不正行為が確認され、また処理（この例の場合、決済処理）が成功したか否かが確認され（ステップ S 8 0 7）、それらの確認結果に基づいて、登録リストが更新される。さらに、このようにして更新された登録リストは、各レシーバに保持されるようにしたので、各レシーバの動作を制御することができる。

【0262】

以上においては、ステップ S 3 5 5 において、計上された課金が予め設定された上限額を超えた場合、ステップ S 3 5 6 に進み、配送用鍵 K d の受け取り処理が実行されるようにしたが、購入されるコンテンツの個数の上限数を設定し、購入されたコンテンツの個数がその上限数を超えた場合においても、ステップ S 3 5 6 に進むようにすることもできる。

【0263】

また、以上においては、課金処理における場合を例として、登録リストの利用方法を説明したが、コンテンツが復号される場合、取扱方針に含まれるコンテンツ鍵 K c o のバージョンが、レシーバ 5 1 の SAM 6 2 で保持される配送用鍵 K d のバージョンより新しいときなども、登録リストがレシーバ 5 1 より EMD サービスセンタ 1 に送信される。この場合においても、登録リストは、上述したように、EMD サービスセンタ 1 において作成され、各レシーバにおいて配布される。

【0264】

また、以上においては、機器（例えば、レシーバ 5 1、またはレシーバ 2 0 1）が接続されるタイミングで、登録リストが課金情報とともに EMD サービスセンタ 1 に送信される場合を例として説明したが、このとき登録リストのみが送信されるようにすることもできる。また、以上においては、機器が登録されるときに課金情報が、EMD サービスセンタ 1 に送信される場合を例として説明したが、そ

れ以外のタイミングで課金情報をEMDサービスセンタ1に送信するようにしてもよい。

【0265】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【0266】

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【0267】

【発明の効果】

請求項1に記載の管理装置、請求項4に記載の管理方法、および請求項5に記載の提供媒体によれば、情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録するようにしたので、迅速にユーザの契約の可否が判断できるようになる。

【0268】

請求項6に記載の情報処理装置、請求項8に記載の情報処理方法、および請求項9に記載の提供媒体によれば、情報処理装置に従属する他の情報処理装置の登録を請求するようにしたので、複数の情報処理装置を有するユーザも簡単に契約の処理ができるようになる。

【0269】

請求項10に記載のシステムによれば、管理装置が、情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録し、情報処理装置が、情報処理装置に従属する他の情報処理装置の登録を請求するようにしたので、迅速にユーザの契約の可否が判断でき、複数の情報処理装置を有するユーザも簡単に契約の処理ができるようになる。

【0270】

請求項11に記載の情報処理装置、請求項12に記載の情報処理方法、および請求項13に記載の提供媒体によれば、登録条件を記憶するようにしたので、違

反などがあつた場合の動作を簡単かつ確実に制御（制限）することができる。

【0271】

請求項 14 に記載の管理装置、請求項 15 に記載の管理方法、および請求項 16 に記載の提供媒体によれば、所定の処理を実行するとき、登録条件を作成するようにしたので、違反などがあつた場合の情報処理装置の動作を簡単にかつ確実に制御（制限）することができる。

【図面の簡単な説明】

【図 1】

EMD のシステムを説明する図である。

【図 2】

EMD サービスセンタ 1 の機能の構成を示すブロック図である。

【図 3】

EMD サービスセンタ 1 の配送用鍵 K d の送信を説明する図である。

【図 4】

EMD サービスセンタ 1 の配送用鍵 K d の送信を説明する図である。

【図 5】

EMD サービスセンタ 1 の配送用鍵 K d の送信を説明する図である。

【図 6】

EMD サービスセンタ 1 の配送用鍵 K d の送信を説明する図である。

【図 7】

ユーザ登録データベースを説明する図である。

【図 8】

コンテンツプロバイダ 2 の機能の構成を示すブロック図である。

【図 9】

サービスプロバイダ 3 の機能の構成を示すブロック図である。

【図 10】

ユーザホームネットワーク 5 の構成を示すブロック図である。

【図 11】

ユーザホームネットワーク 5 の構成を示すブロック図である。

【図 12】

コンテンツおよびコンテンツに付随する情報を説明する図である。

【図 13】

コンテンツプロバイダセキュアコンテナを説明する図である。

【図 14】

コンテンツプロバイダ 2 の証明書を説明する図である。

【図 15】

サービスプロバイダセキュアコンテナを説明する図である。

【図 16】

サービスプロバイダ 3 の証明書を説明する図である。

【図 17】

取扱方針、価格情報、および使用許諾条件情報を示す図である。

【図 18】

シングルコピーおよびマルチコピーを説明する図である。

【図 19】

取扱方針および価格情報を説明する図である。

【図 20】

取扱方針、価格情報、および使用許諾条件情報を説明する図である。

【図 21】

コンテンツおよびコンテンツに付随する情報の他の構成を説明する図である。

【図 22】

サービスプロバイダセキュアコンテナを説明する図である。

【図 23】

取扱方針、取扱制御情報、価格情報、及び使用許諾条件の構成を示す図である。

【図 24】

コンテンツおよびコンテンツに付随する情報の他の構成を説明する図である。

【図 25】

コンテンツプロバイダセキュアコンテナを説明する図である。

【図 26】

サービスプロバイダセキュアコンテナを説明する図である。

【図 27】

EMDサービスセンタ 1 の、ユーザホームネットワーク 5 からの課金情報の受信のときの動作を説明する図である。

【図 28】

EMDサービスセンタ 1 の利益分配処理の動作を説明する図である。

【図 29】

EMDサービスセンタ 1 の、コンテンツの利用実績の情報をJASRACに送信する処理の動作を説明する図である。

【図 30】

コンテンツの配布の処理を説明するフローチャートである。

【図 31】

コンテンツの配布の処理を説明するフローチャートである。

【図 32】

EMDサービスセンタ 1 がコンテンツプロバイダ 2 へ配送用鍵 K d を送信する処理を説明するフローチャートである。

【図 33】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

【図 34】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

【図 35】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

【図 36】

レシーバ 5 1 の EMD サービスセンタ 1 への登録の処理を説明するフローチャートである。

【図 3 7】

SAMの証明書を説明する図である。

【図 3 8】

登録リストを説明する図である。

【図 3 9】

ICカード 5 5 への SAM 6 2 のデータのバックアップの処理を説明するフローチャートである。

【図 4 0】

ICカード 5 5 への SAM 6 2 のデータのバックアップの処理を説明するフローチャートである。

【図 4 1】

新しいレシーバに IC カード 5 5 のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図 4 2】

新しいレシーバに IC カード 5 5 のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図 4 3】

新しいレシーバに IC カード 5 5 のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図 4 4】

レシーバ 5 1 が、従属関係のあるレコーダ 5 3 を EMD サービスセンタ 1 に登録する処理を説明するフローチャートである。

【図 4 5】

レシーバ 5 1 が EMD サービスセンタ 1 から配送用鍵 K d を受け取る処理を説明するフローチャートである。

【図 4 6】

レコーダの配送用鍵 K d の受け取り処理を説明するフローチャートである。

【図 4 7】

コンテンツプロバイダ 2 がサービスプロバイダ 3 にコンテンツプロバイダセキ

ユアコンテナを送信する処理を説明するフローチャートである。

【図48】

コンテンツプロバイダ2がサービスプロバイダ3にコンテンツプロバイダセキ
ユアコンテナを送信する他の処理を説明するフローチャートである。

【図49】

サービスプロバイダ3がレシーバ51にサービスプロバイダセキユアコンテナ
を送信する処理を説明するフローチャートである。

【図50】

サービスプロバイダ3がレシーバ51にサービスプロバイダセキユアコンテナ
を送信する処理を説明するフローチャートである。

【図51】

レシーバ51の課金処理を説明するフローチャートである。

【図52】

レシーバ51がコンテンツを再生する処理を説明するフローチャートである。

【図53】

レシーバ51がデコーダ56にコンテンツを再生させる処理を説明するフロー
チャートである。

【図54】

他のEMDシステムを説明する図である。

【図55】

登録リストを説明する他の図である。

【図56】

登録リストを説明する他の図である。

【図57】

登録リストを説明する他の図である。

【図58】

登録リストを保持するための処理を説明するフローチャートである。

【図59】

レシーバ51の登録処理を説明するフローチャートである。

【図 60】

登録リストを説明する他の図である。

【図 61】

レシーバ 201 およびレシーバ 202 の登録処理を説明するフローチャートである。

【図 62】

登録リストを説明する他の図である。

【図 63】

配送用鍵の受け取り処理を説明するフローチャートである。

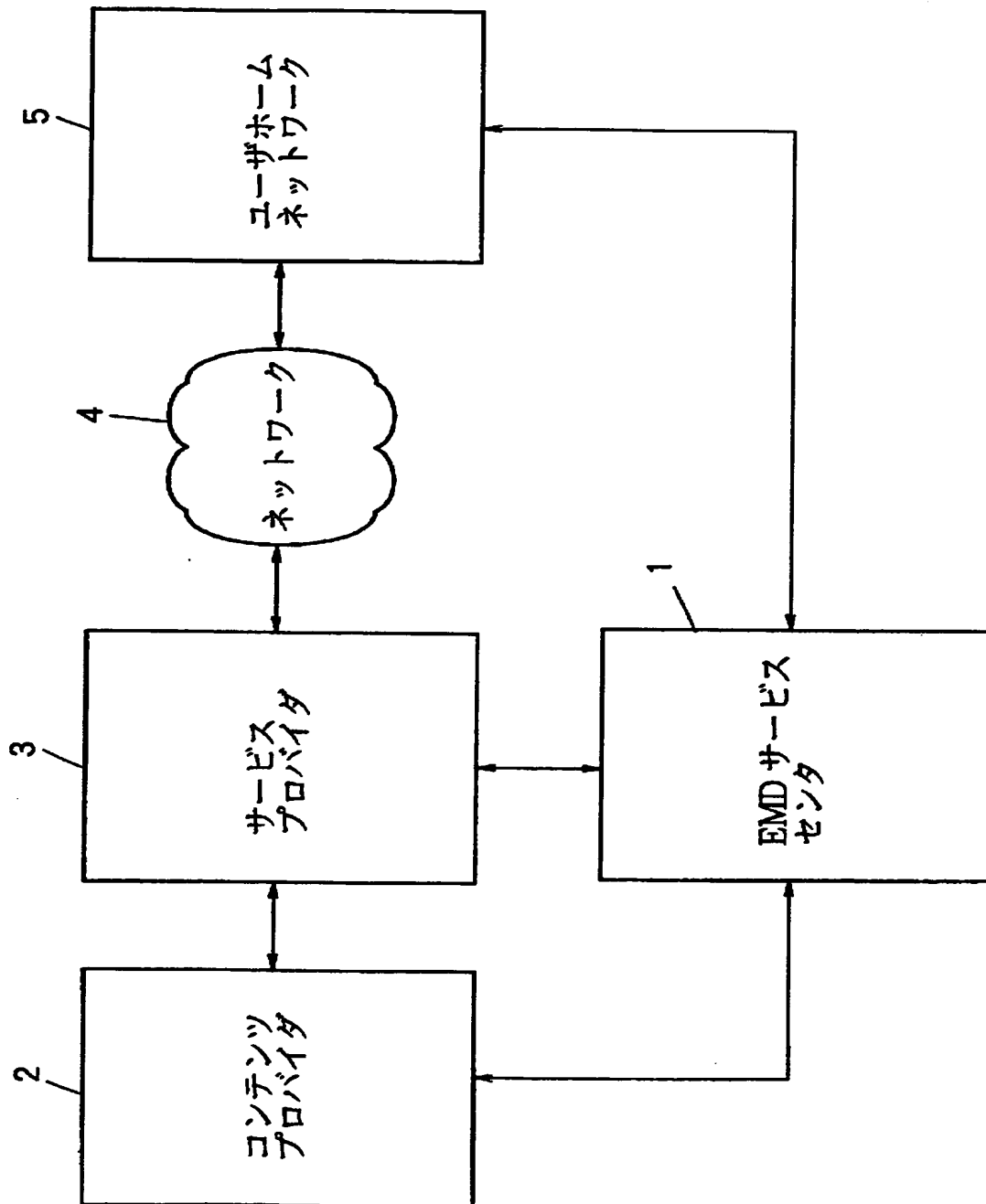
【符号の説明】

1 EMDサービスセンタ, 2 コンテンツプロバイダ, 3 サービスプロバイダ, 5 ユーザホームネットワーク, 16 利益分配部, 18 ユーザ管理部, 42 値付け部, 51 レシーバ, 56 デコーダ, 61 通信部, 62 SAM, 63 伸張部, 71 相互認証モジュール, 72 課金処理モジュール, 73 記憶モジュール, 74 復号/暗号化モジュール, 75 相互認証モジュール, 76 復号モジュール, 77 復号モジュール, 80 相互認証モジュール, 81 記憶モジュール, 91 復号ユニット, 92 乱数発生ユニット, 93 暗号化ユニット, 101 相互認証モジュール, 102 復号モジュール, 103 復号モジュール, 201 レシーバ, 202 レシーバ, 203 HDD, 210 SAM, 211 記憶モジュール, 220 SAM, 221 記憶モジュール

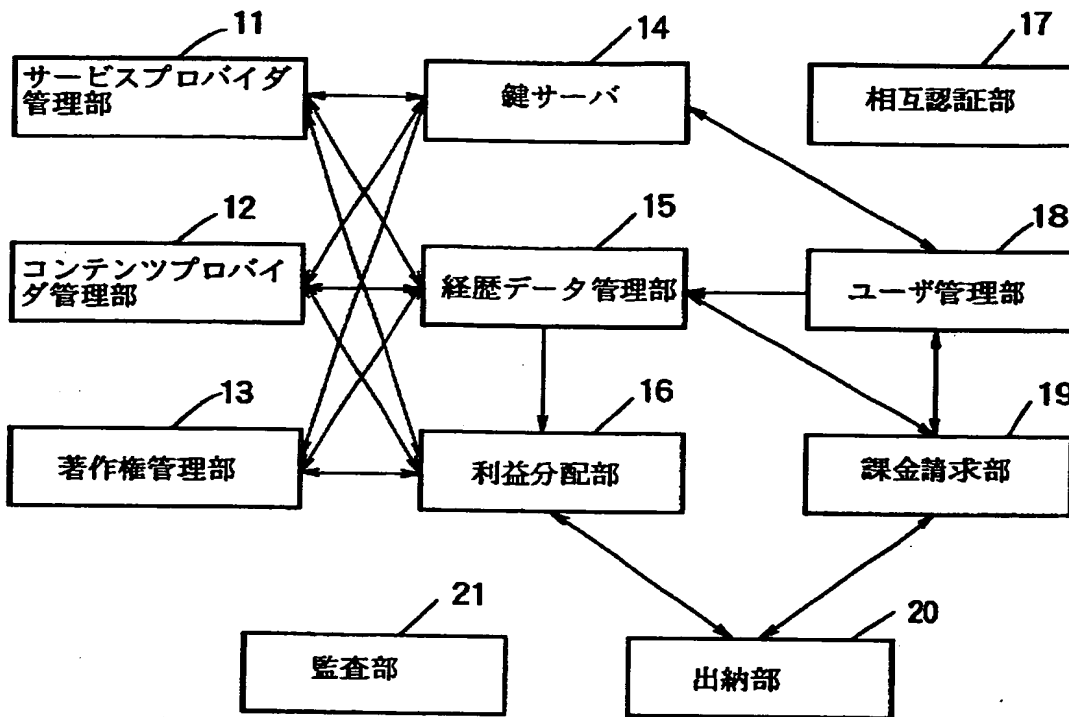
【書類名】

図面

【図 1】

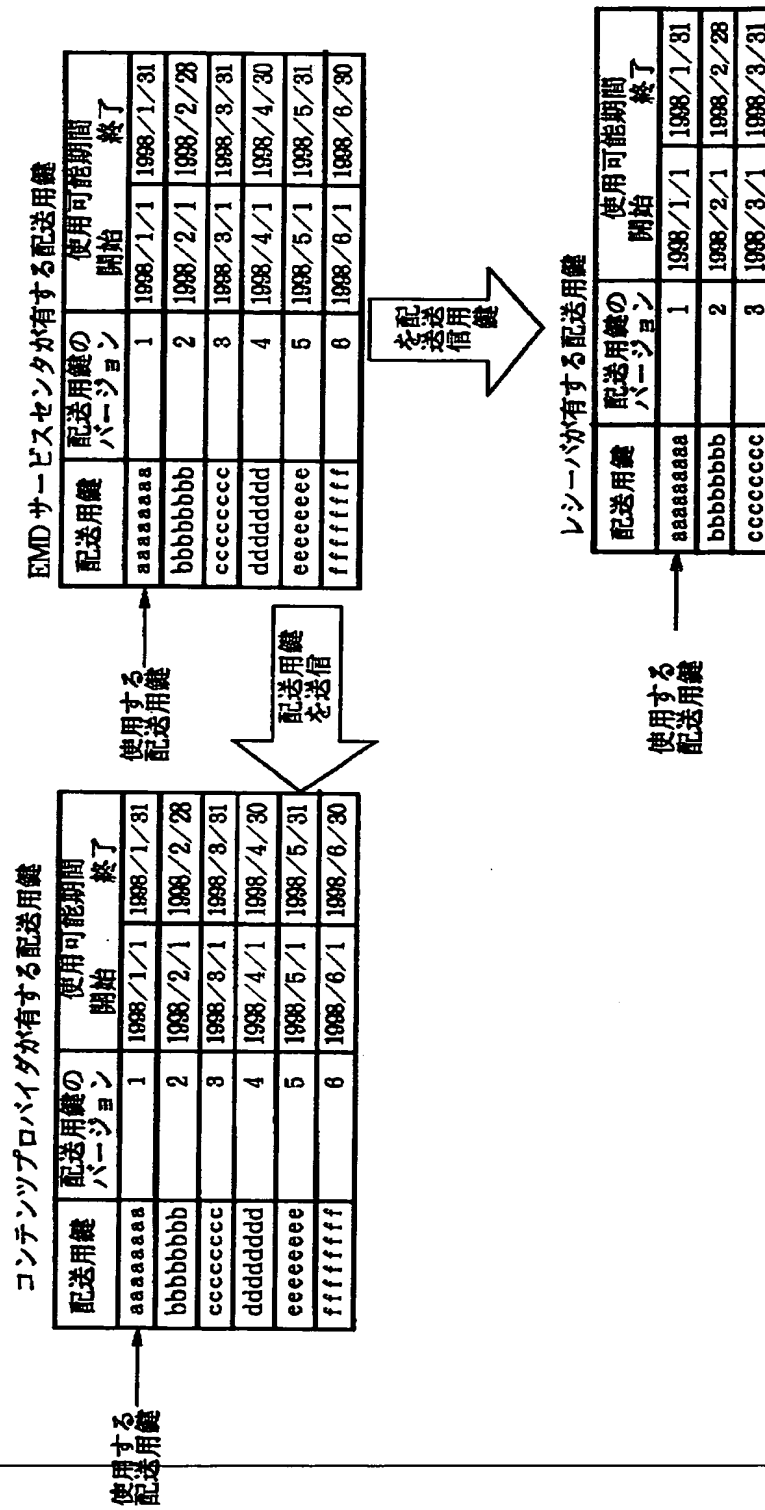


【図 2】

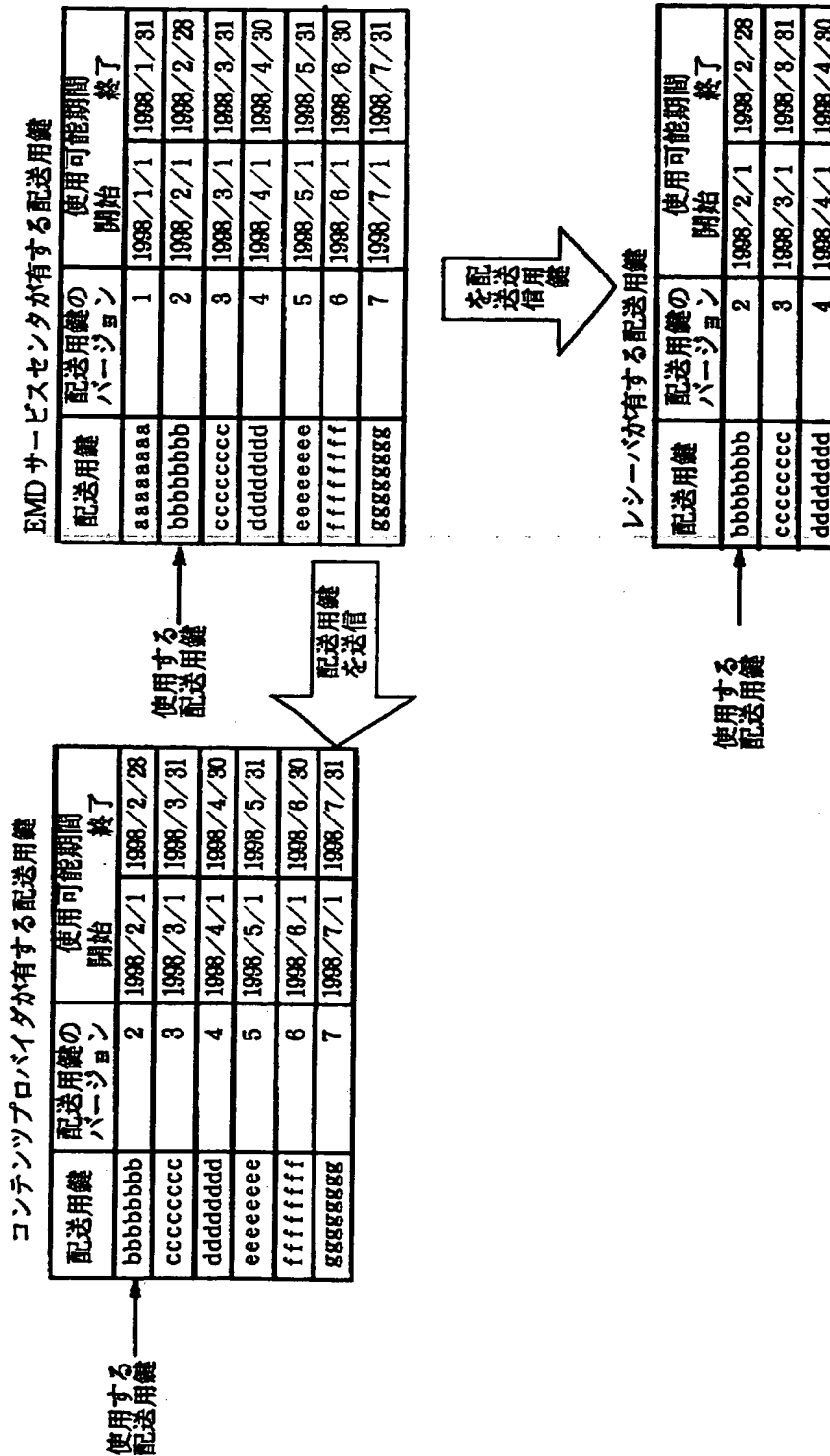


EMD サービスセンタ 1

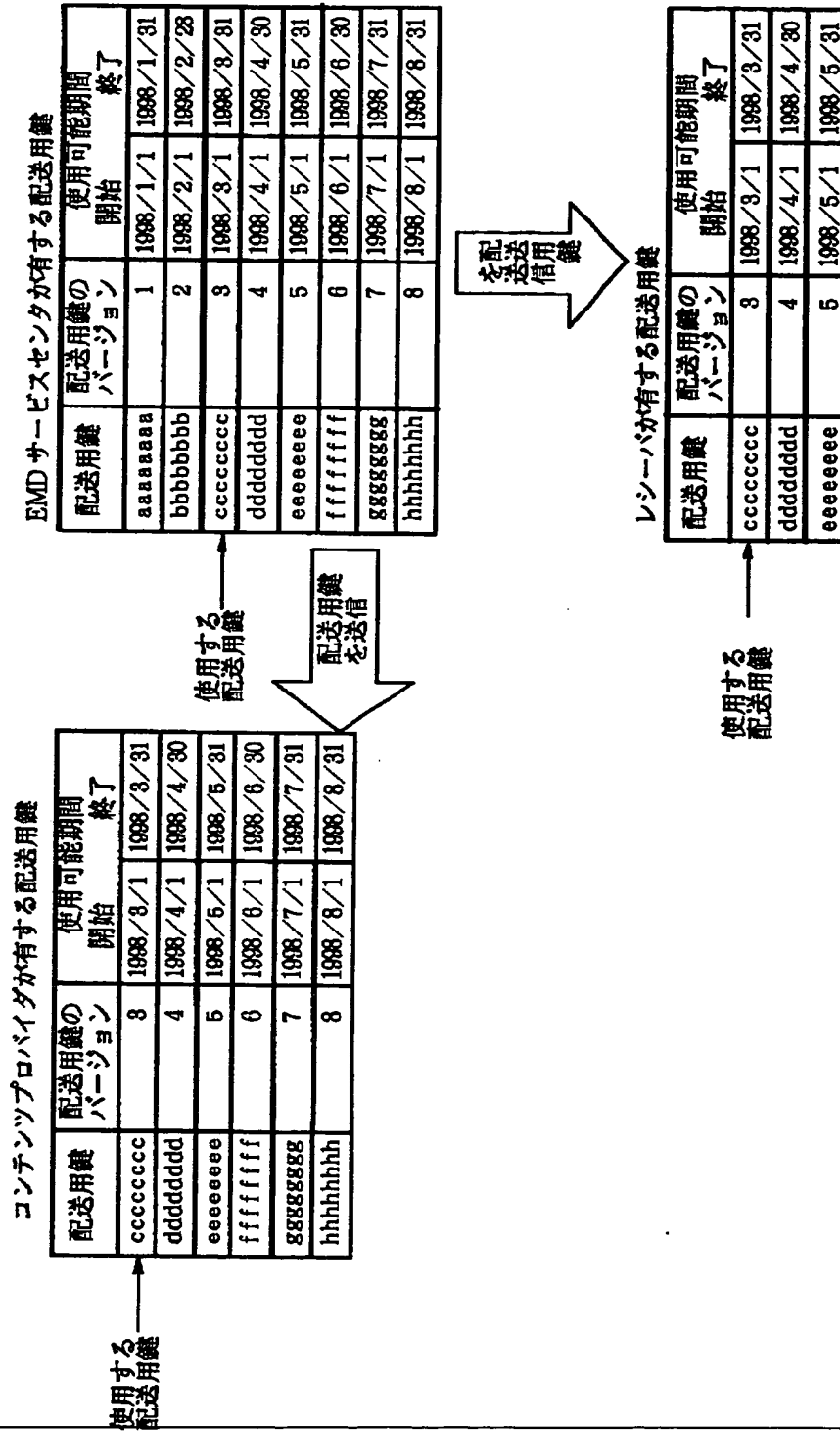
【図 3】



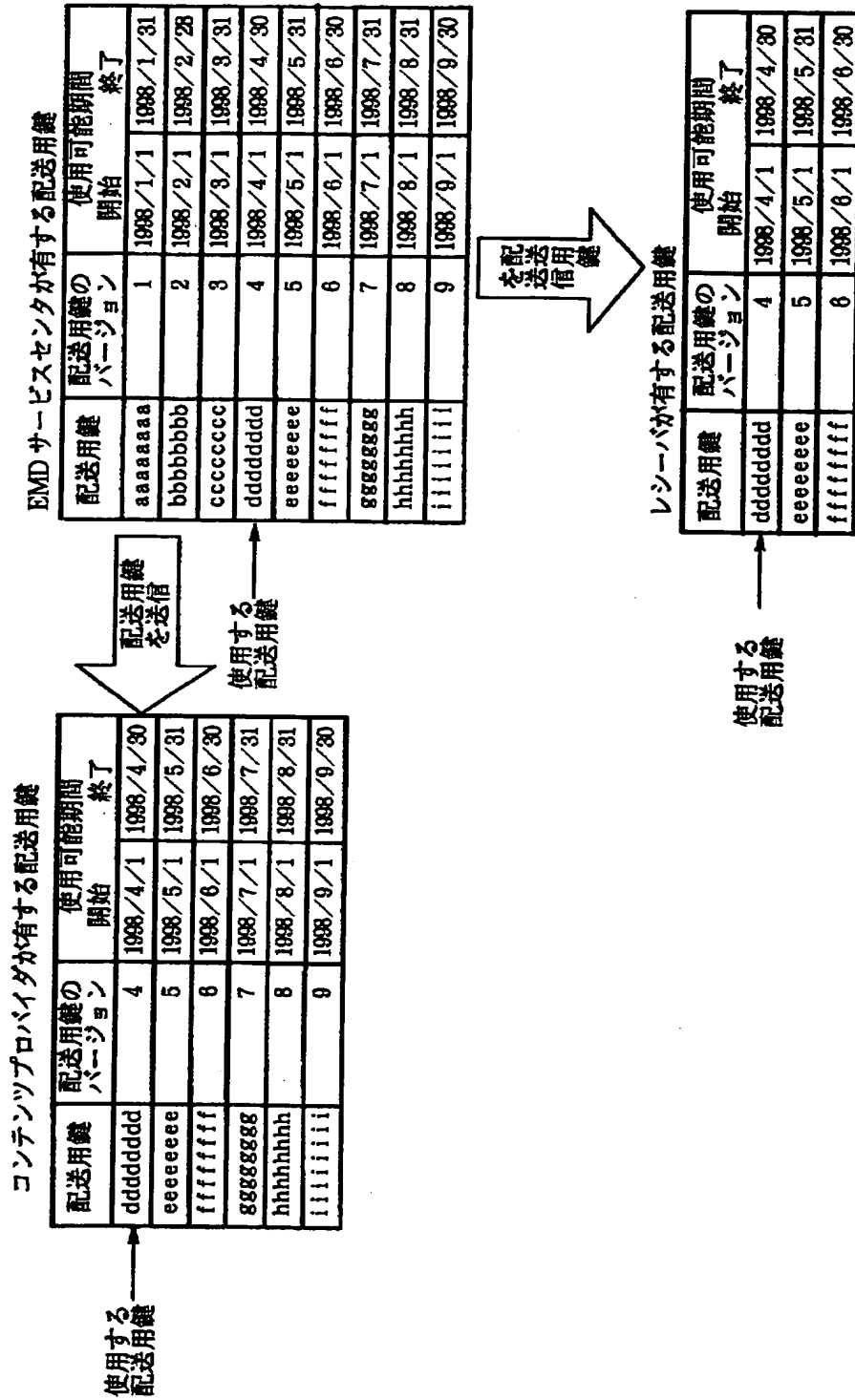
【図 4】



【図 5】



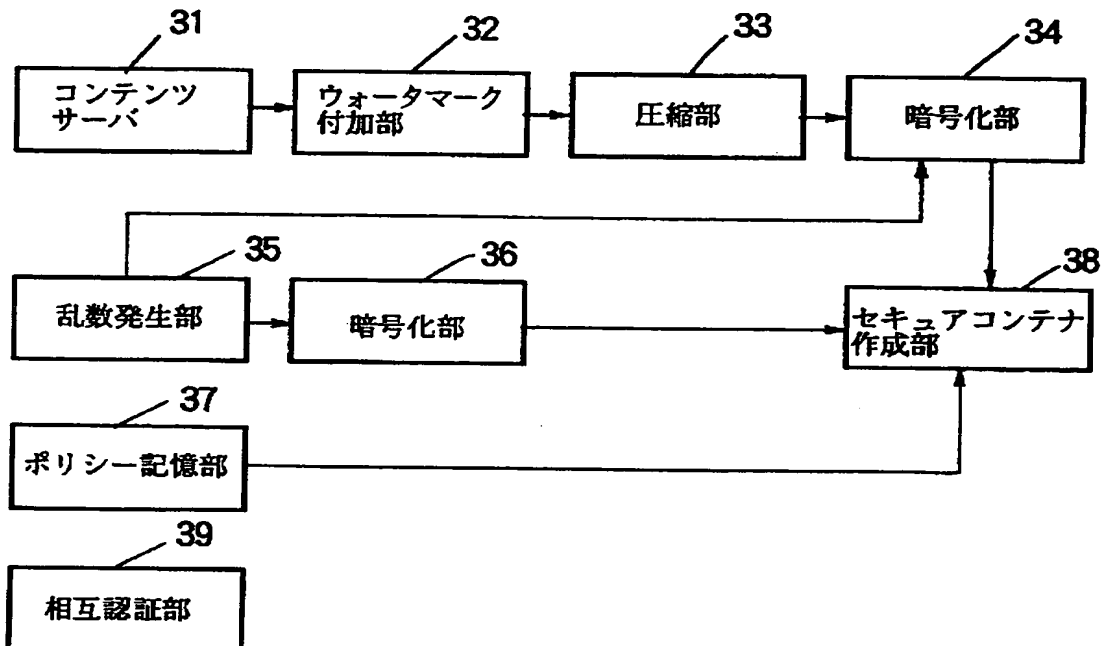
【図 6】



【図 7】

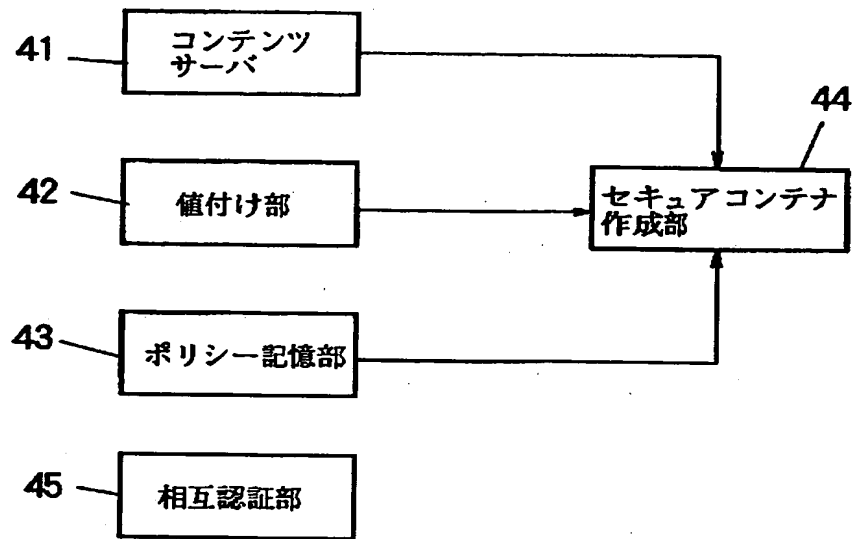
ID	決済処理	登録	EMDサービスセンタとの接続
0000000000000001h	可	可	可
0000000000000002h	可	可	不可
0000000000000003h	可	不可	可
0000000000000004h	可	不可	不可
0000000000000005h	不可	可	可
0000000000000006h	不可	可	不可
0000000000000007h	不可	不可	可
0000000000000008h	不可	不可	不可
0000000000000009h	可	可	可
...			
FFFFFFFFFFFFFFFeh	可	不可	不可
FFFFFFFFFFFFFFFfh	不可	可	可

【図 8】



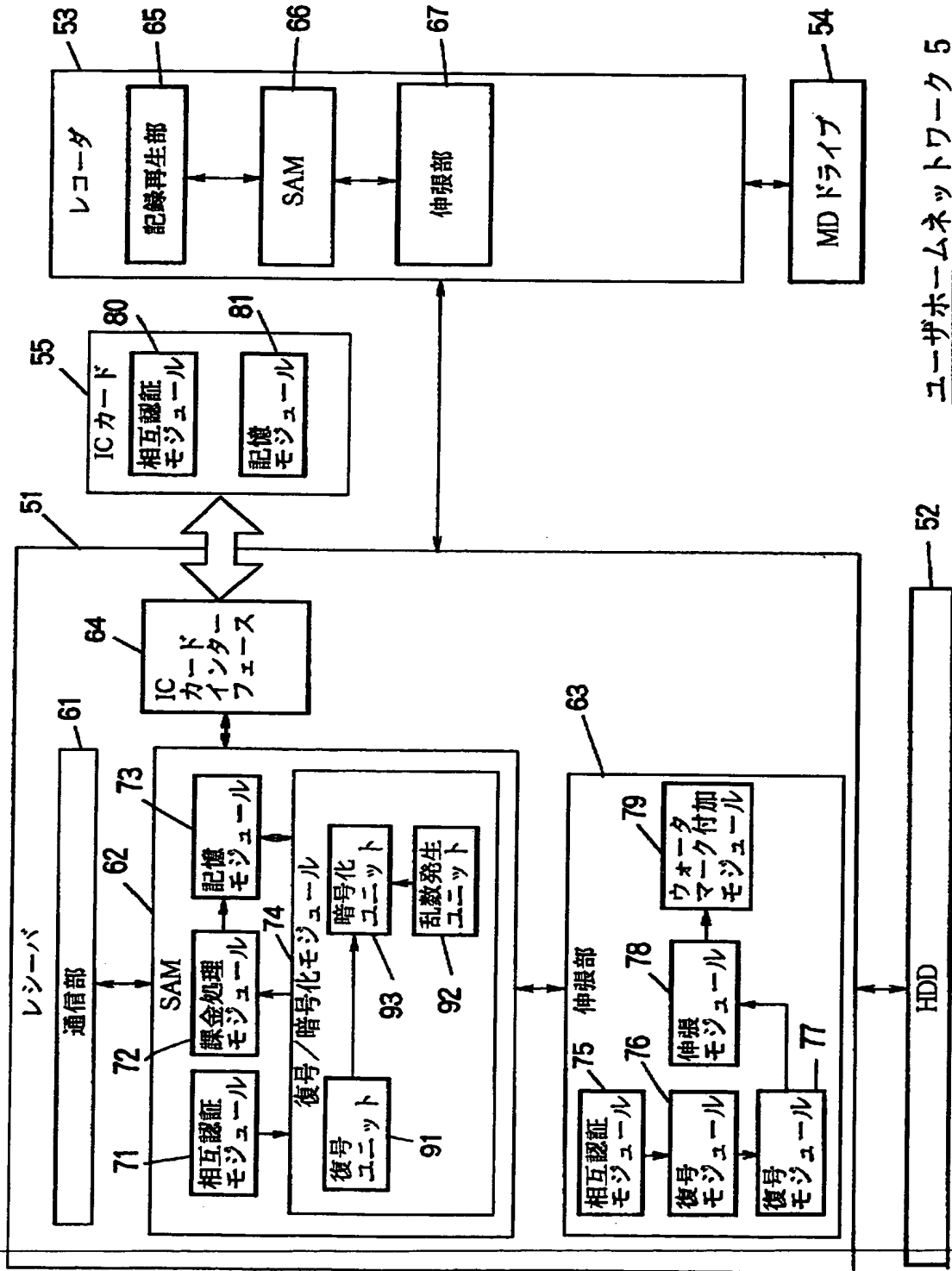
コンテンツプロバイダ 2

【図 9】



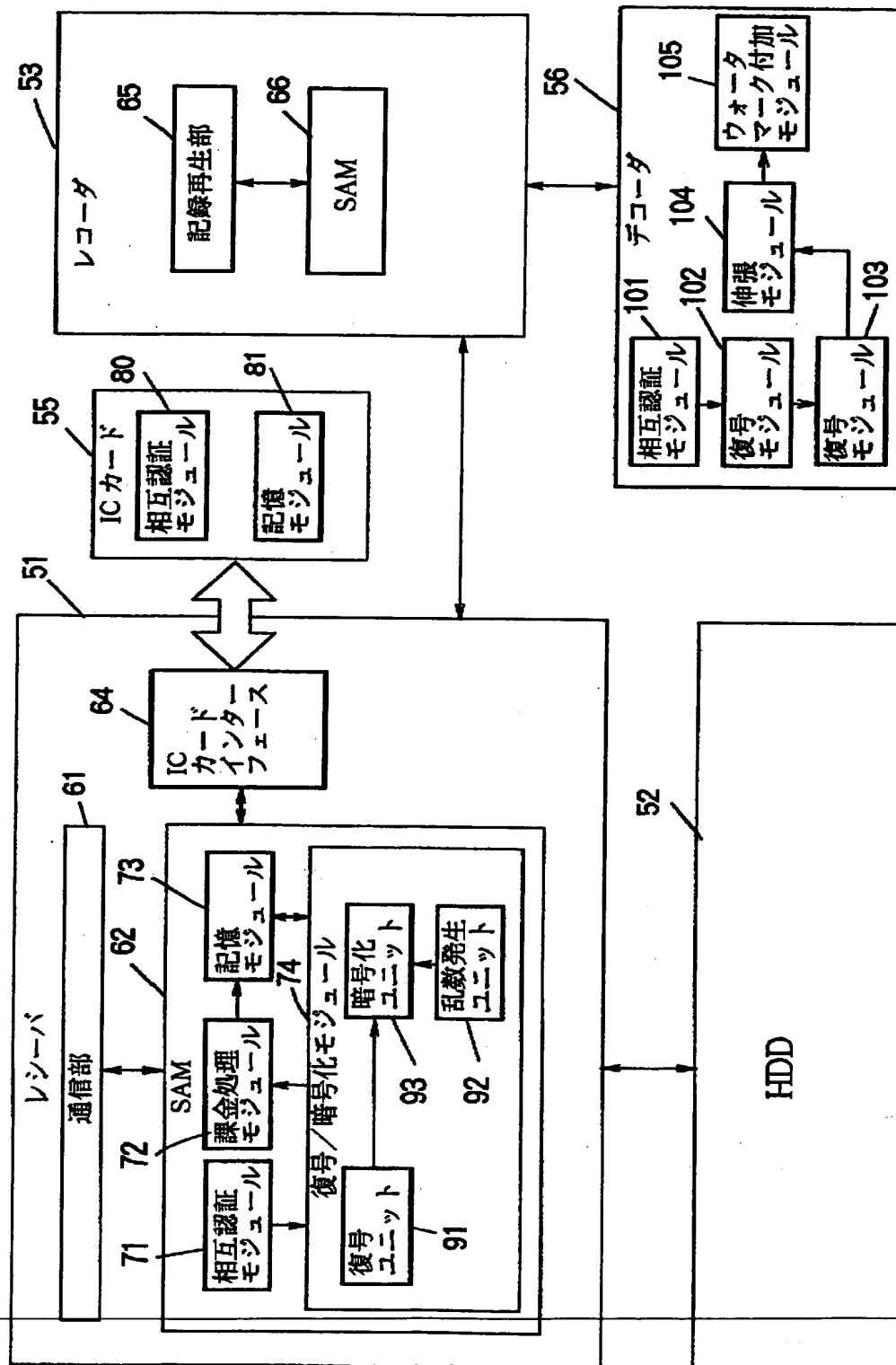
サービスプロバイダ 3

【図 10】



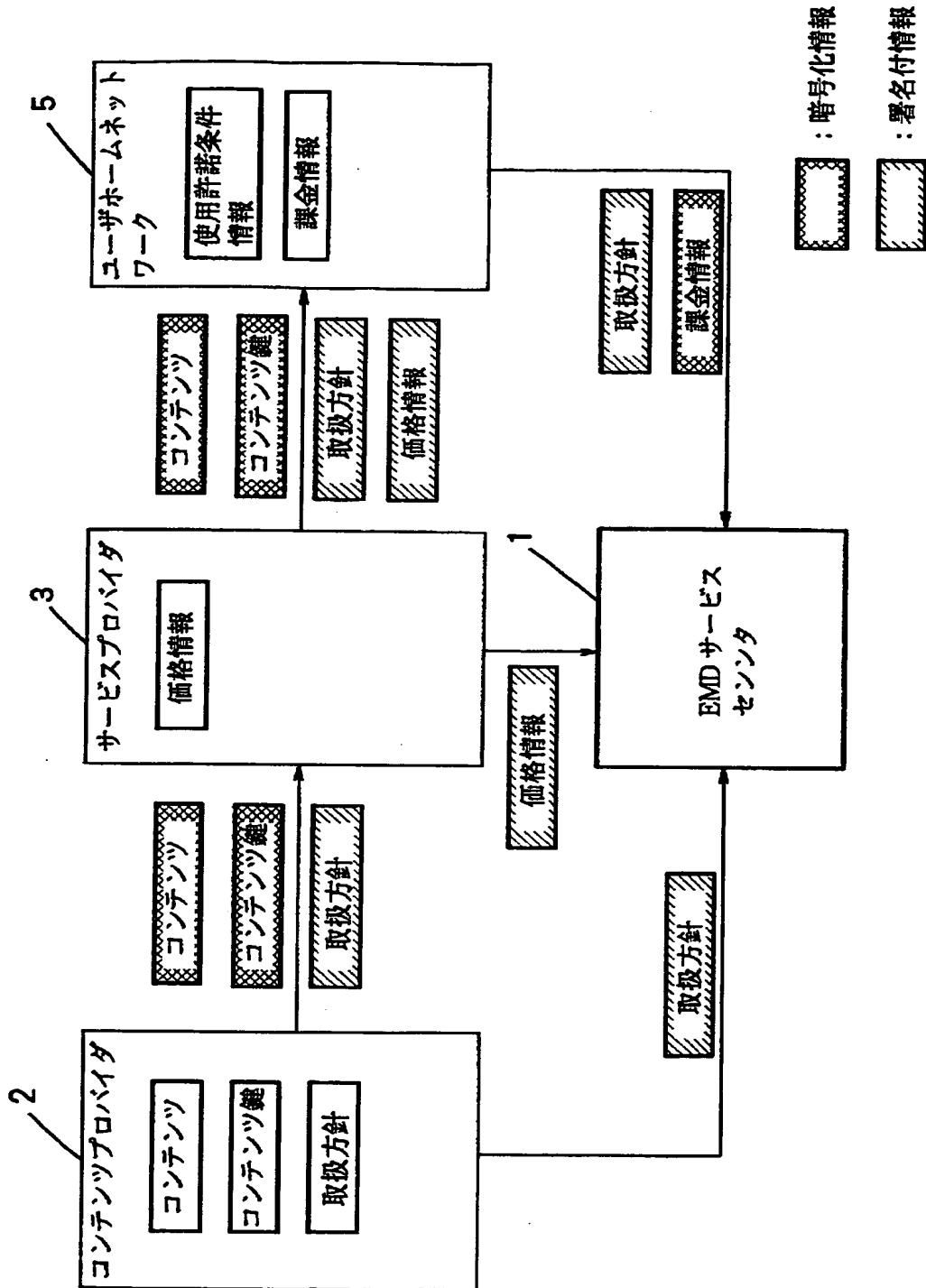
ユーザホームネットワーク 5

【図 11】

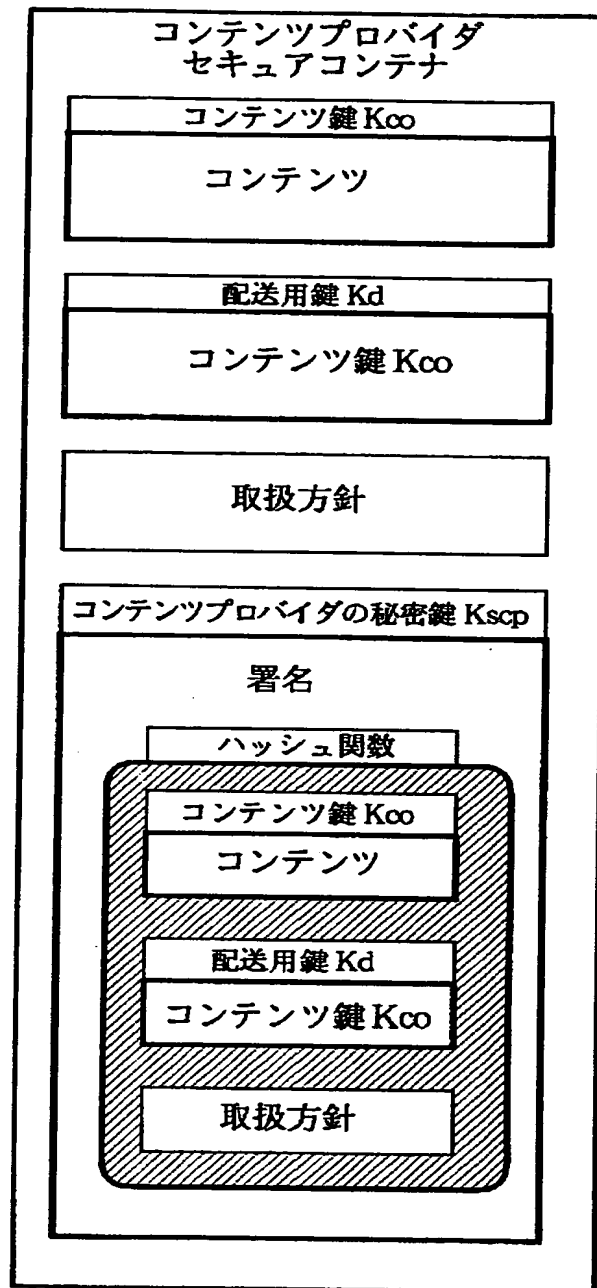


ユーザホームネットワーク 5

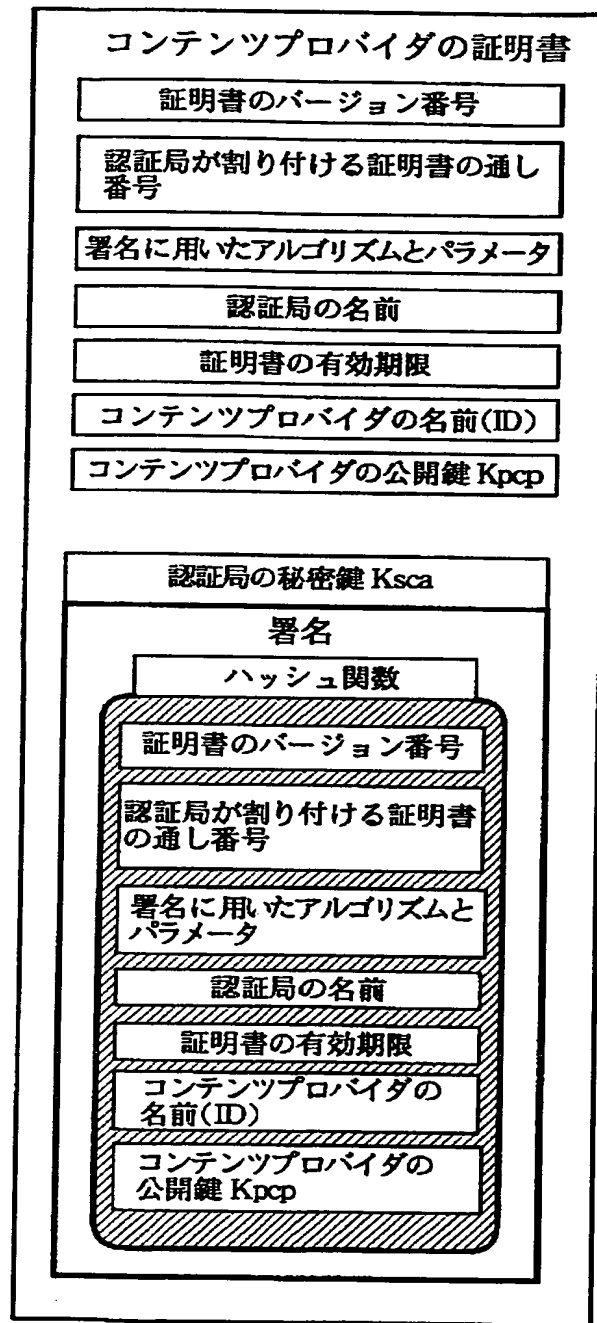
【図 12】



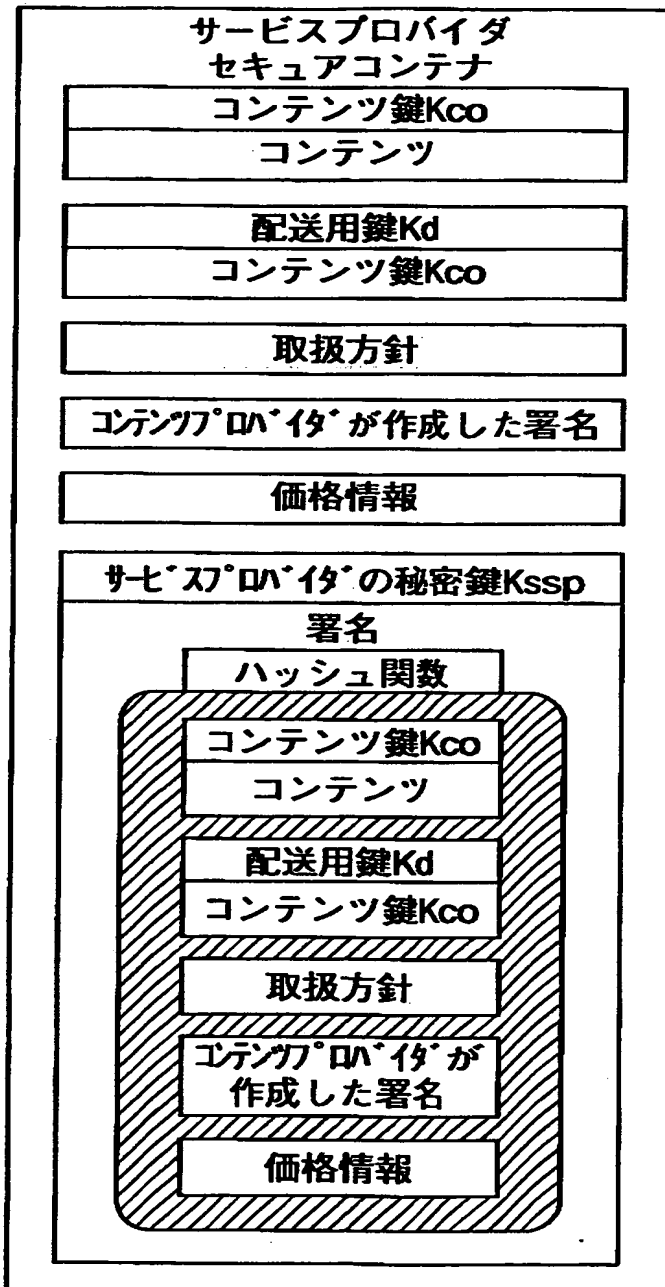
【図 13】



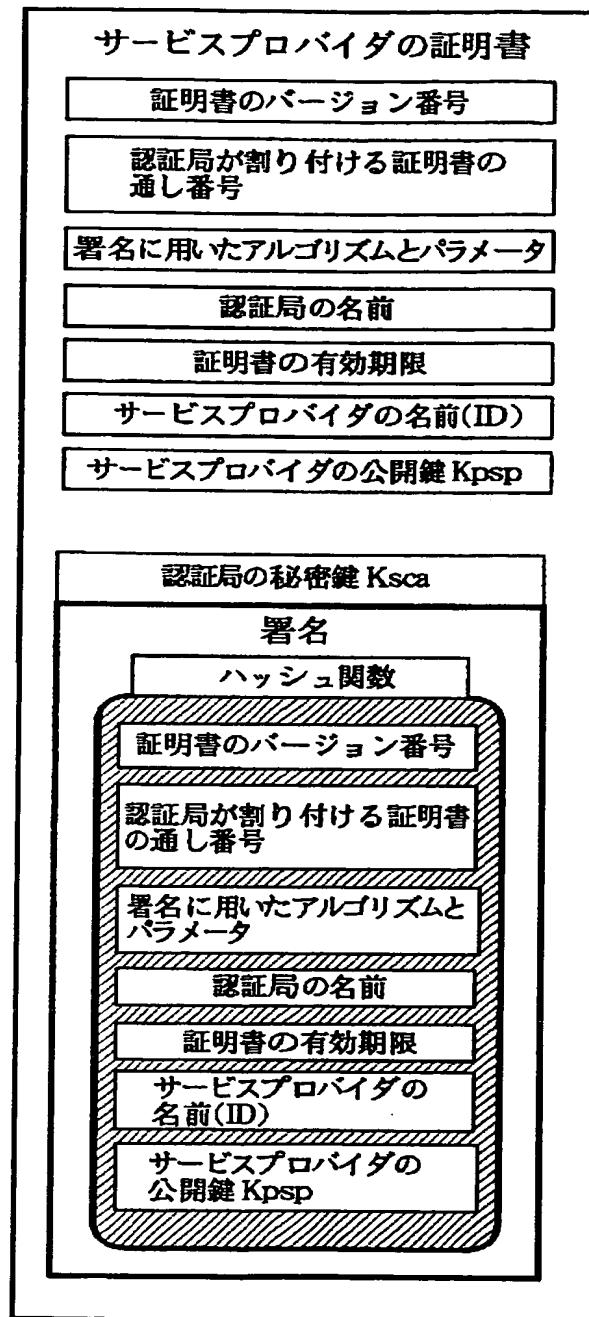
【図 14】



【図 15】



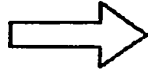
【図 1 6】



【図 17】

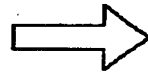
利用内容	再生	シングルコピー	マルチコピー
可/否	1	1	0

(A) 取扱方針



利用内容	再生	シングルコピー	マルチコピー
可/否	1	1	0
価格	150円	80円	-

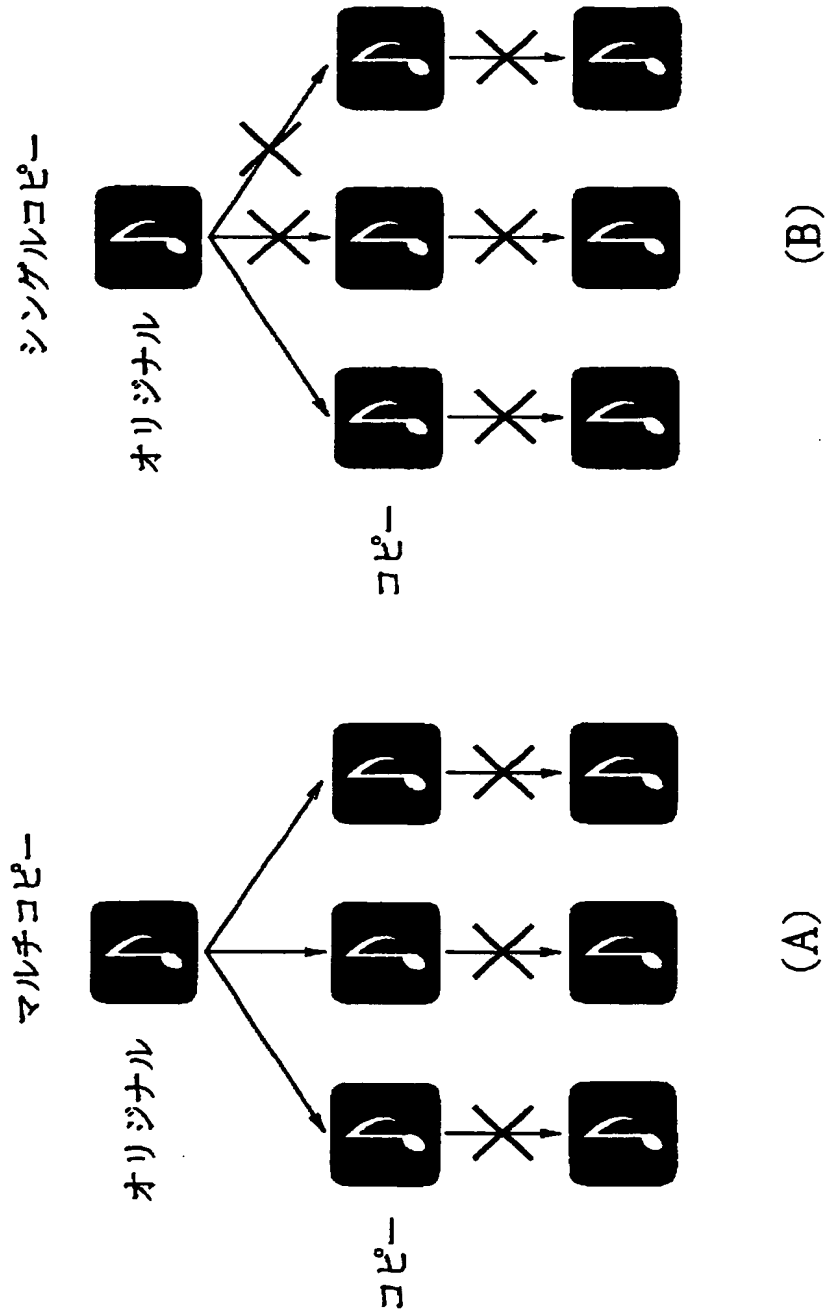
(B) 取扱方針
および
価格情報



利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	0

(C) 使用許諾
条件情報

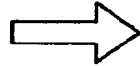
【図 18】



【図 19】

利用内容	再生	シングルコピー	マルチコピー
可/否	1	1	0
利益分配	70円	40円	-

(A) 取扱方針
利益分配



利用内容	再生	シングルコピー	マルチコピー
可/否	1	1	0
利益分配	60円	30円	-
分配価格	150円	80円	-

(B) 取扱方針
利益分配
価格情報



利用内容	再生	シングルコピー	マルチコピー
利用回数	1	0	0

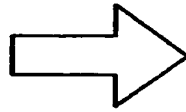
(C) 課金情報

【図 2 0】

利用内容	再生		
	制限なし	回数制限	期日制限
	-	5	1998/12/31
価格	-	60 円	90 円

取扱方針
および
価格情報

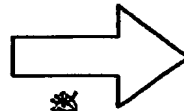
(A)



利用内容	再生		
	制限なし	回数制限	期日制限
	-	5	-

使用許諾条件
情報

(B)



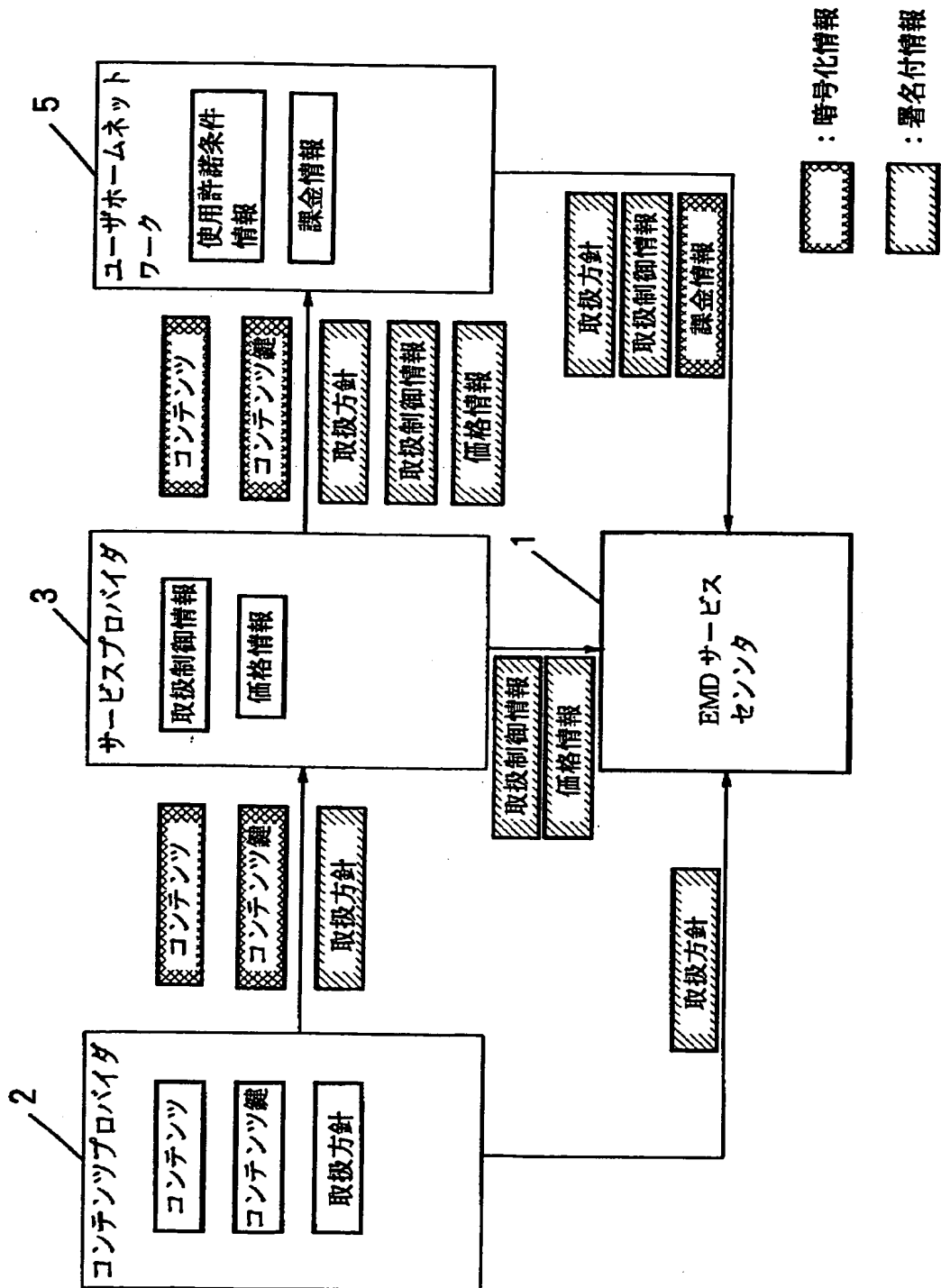
3 回再生後

利用内容	再生		
	制限なし	回数制限	期日制限
	-	2	-

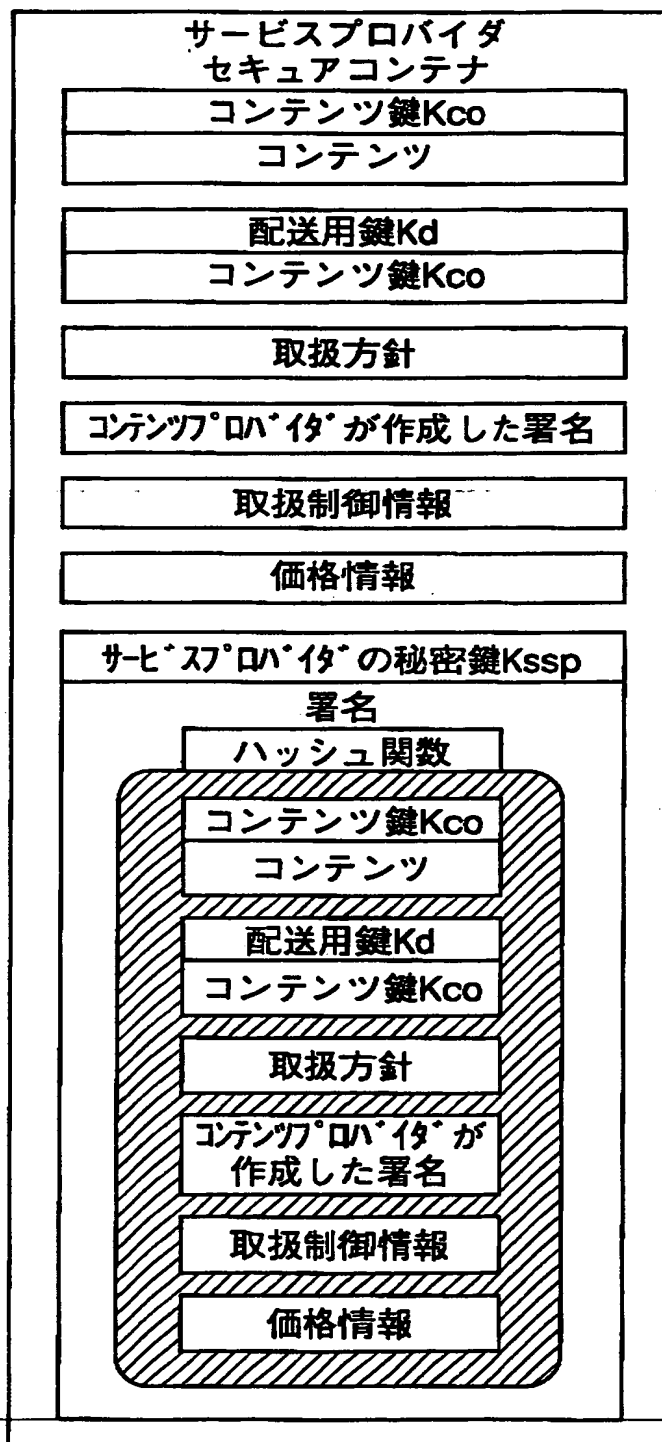
使用許諾条件
情報

(C)

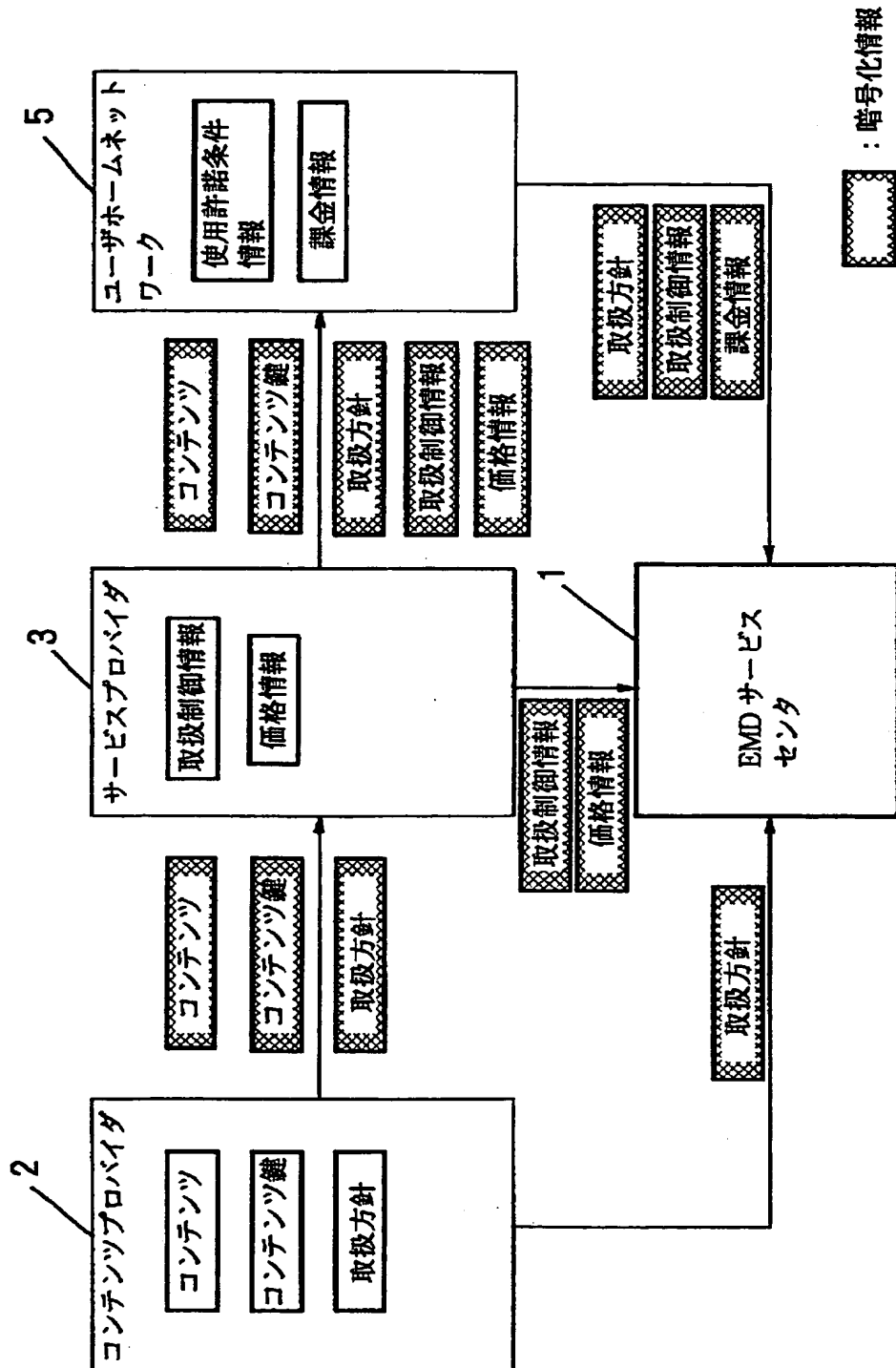
【図 21】



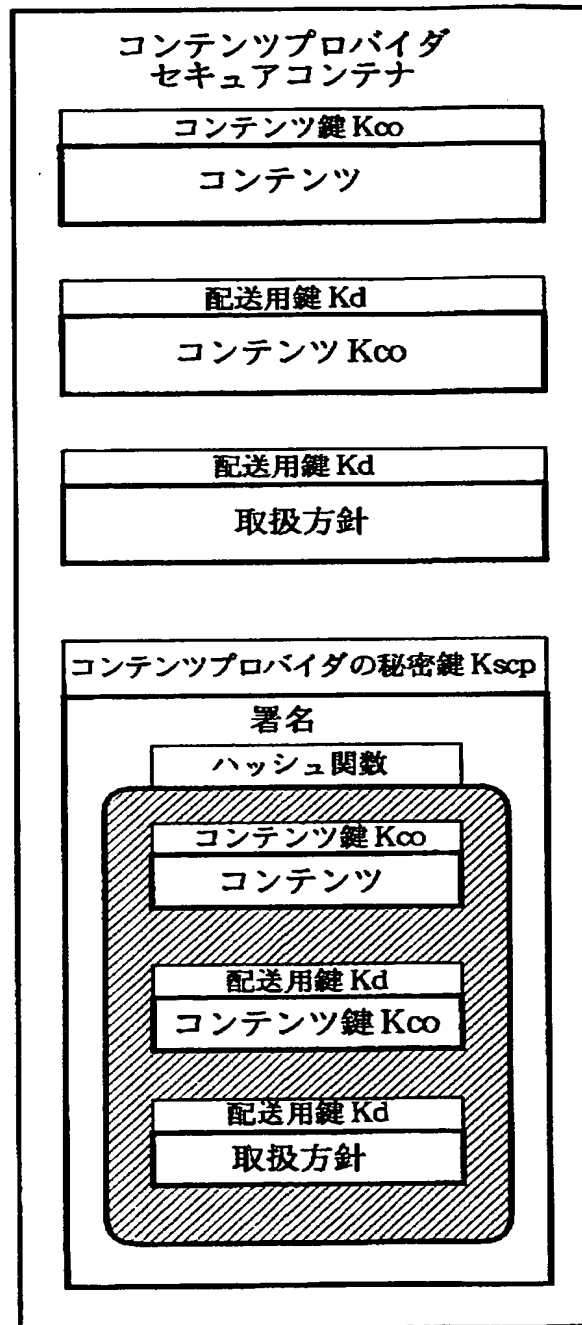
【図 2 2】



【図 24】



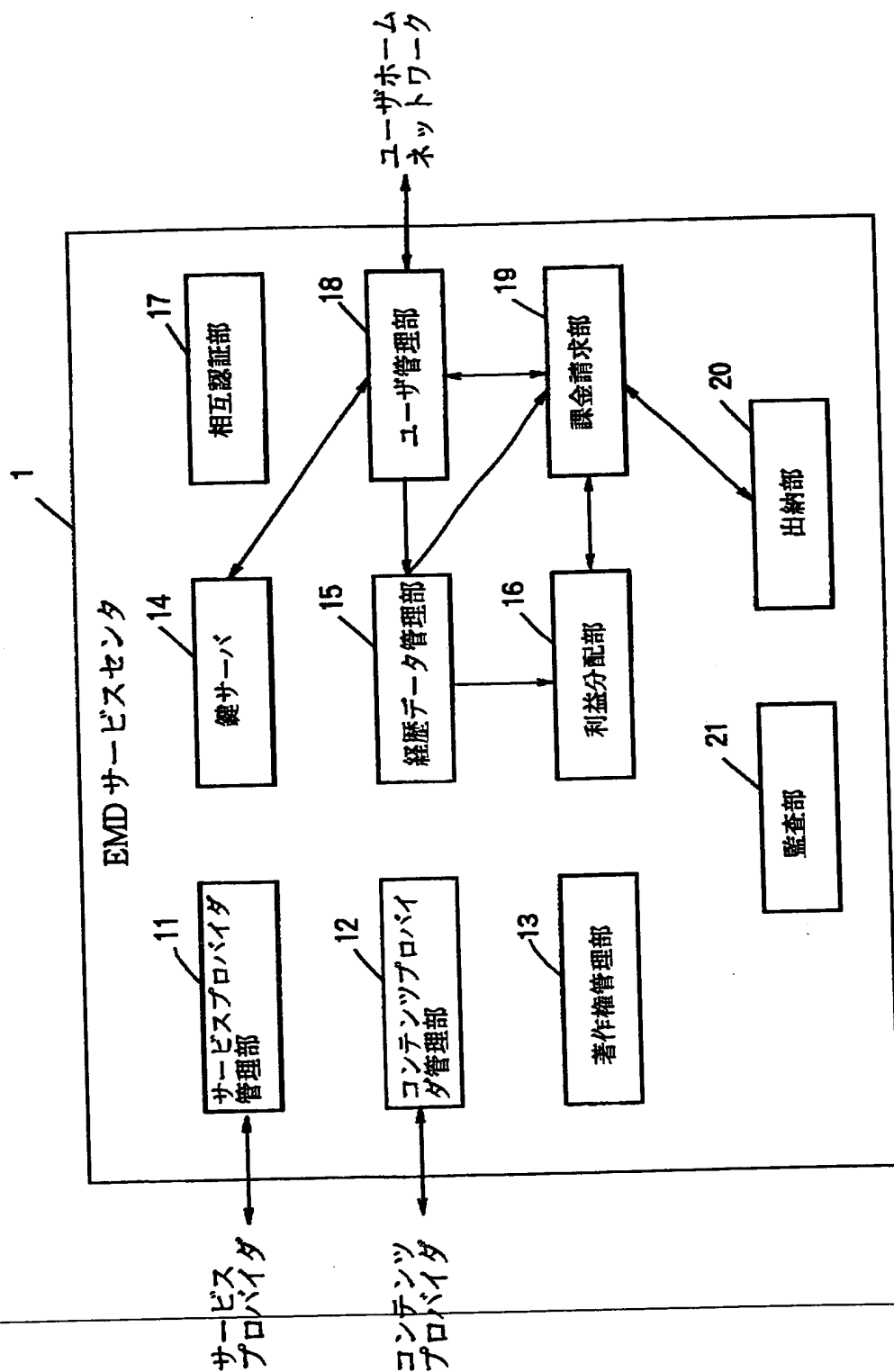
【図 25】



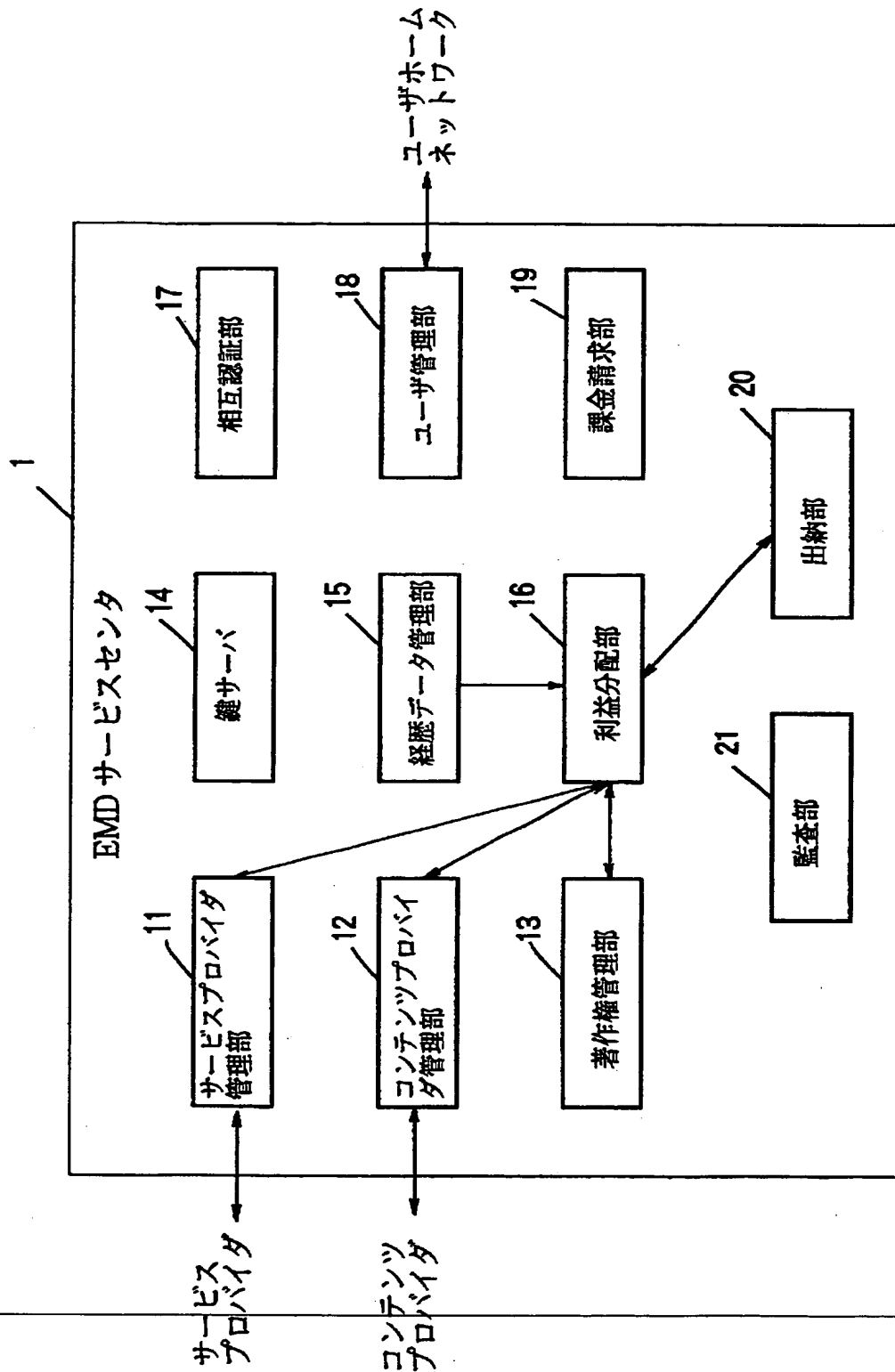
【図 26】



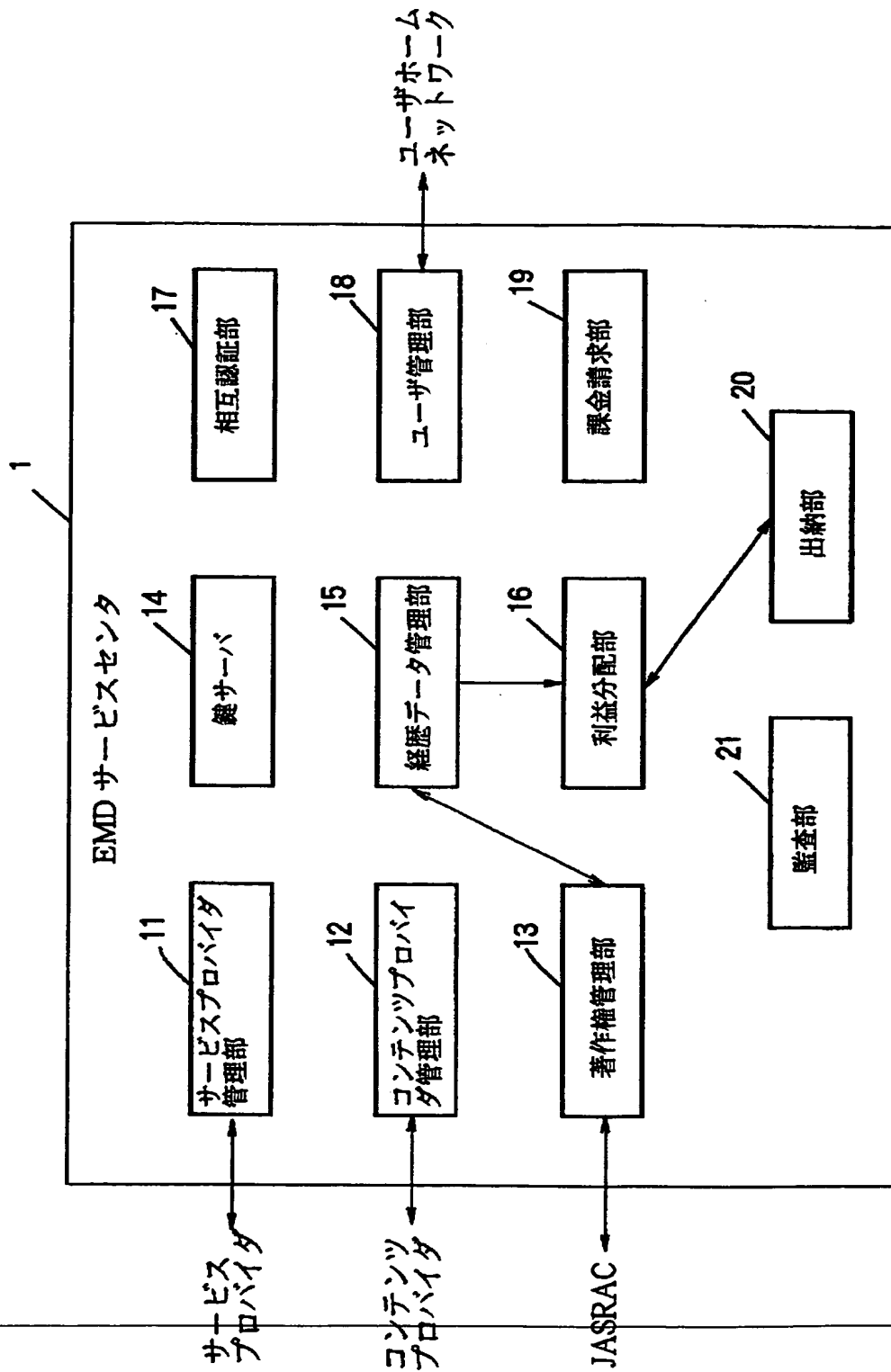
【図 27】



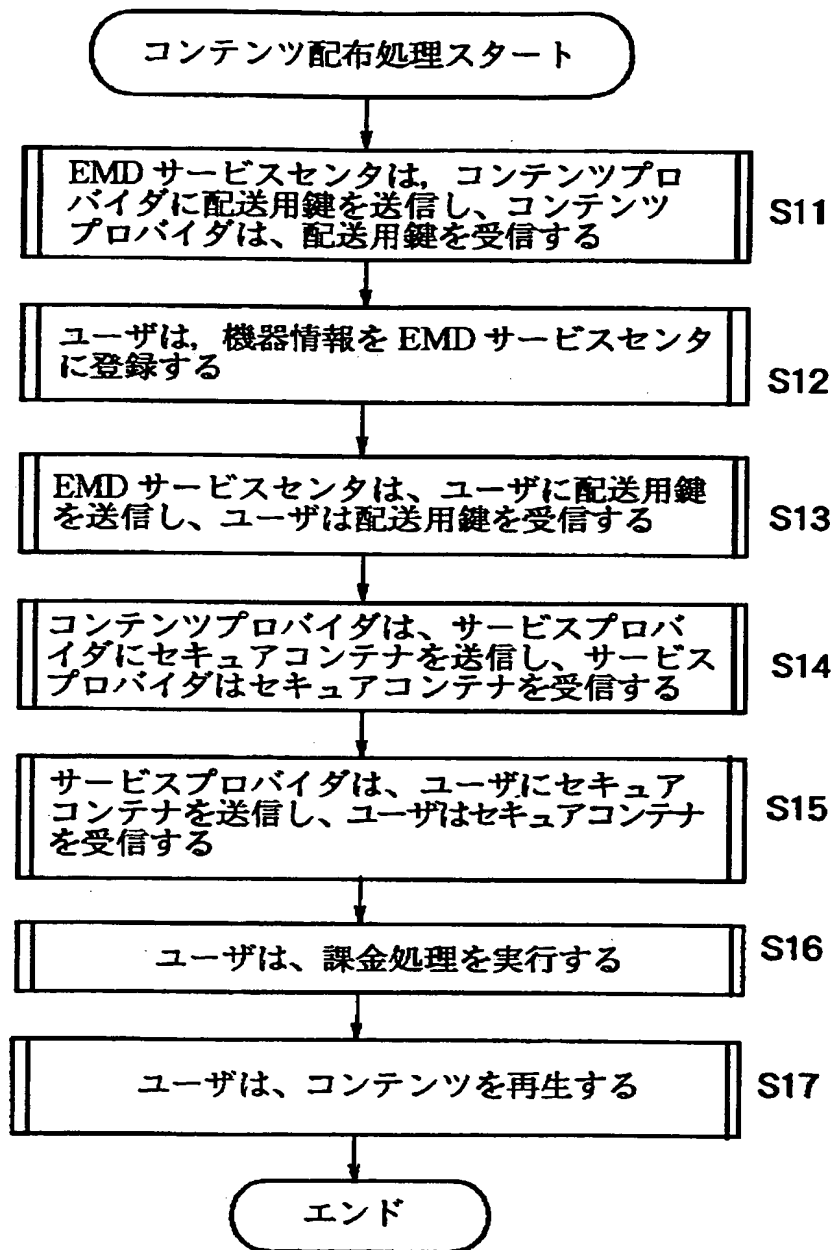
【図 28】



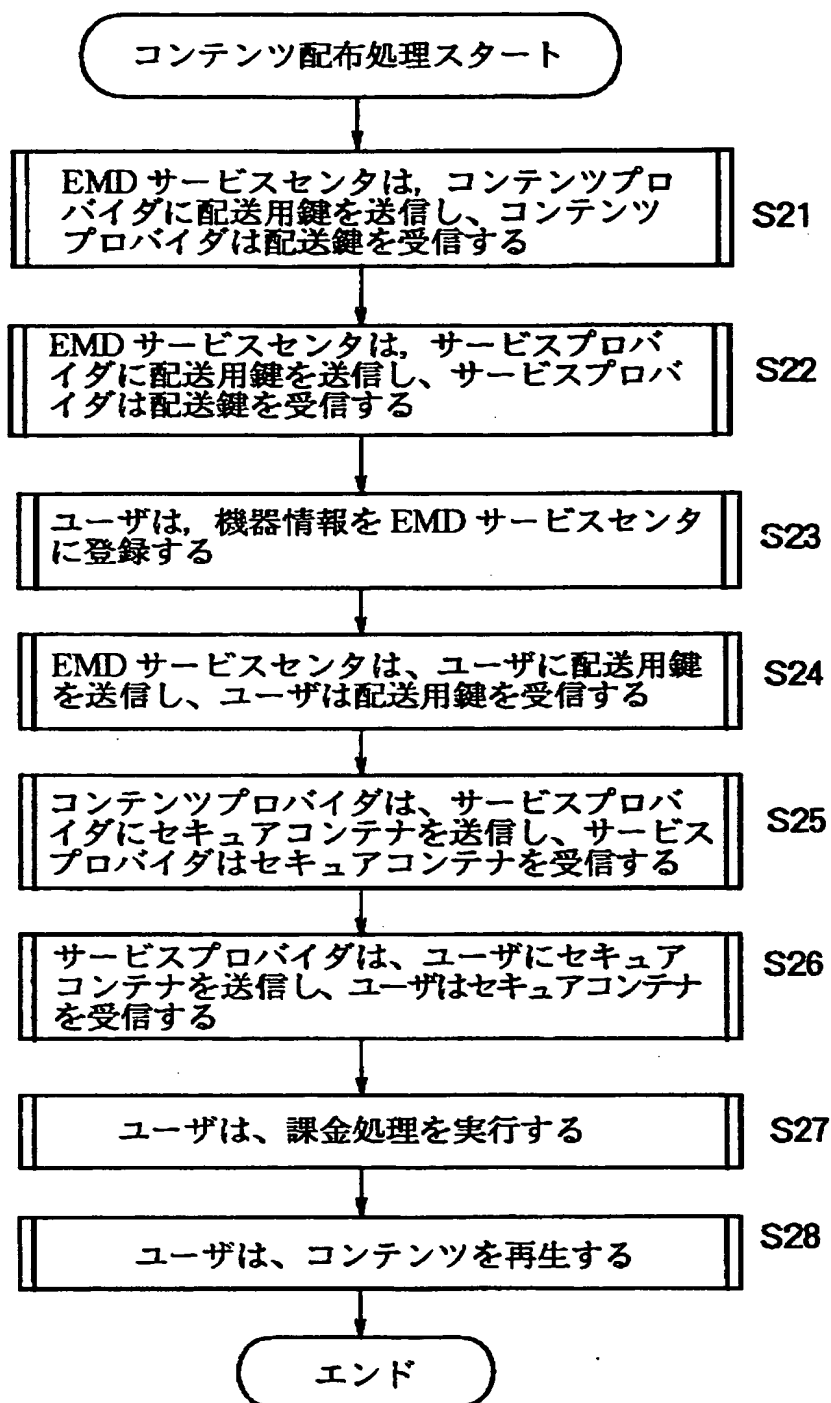
【図 29】



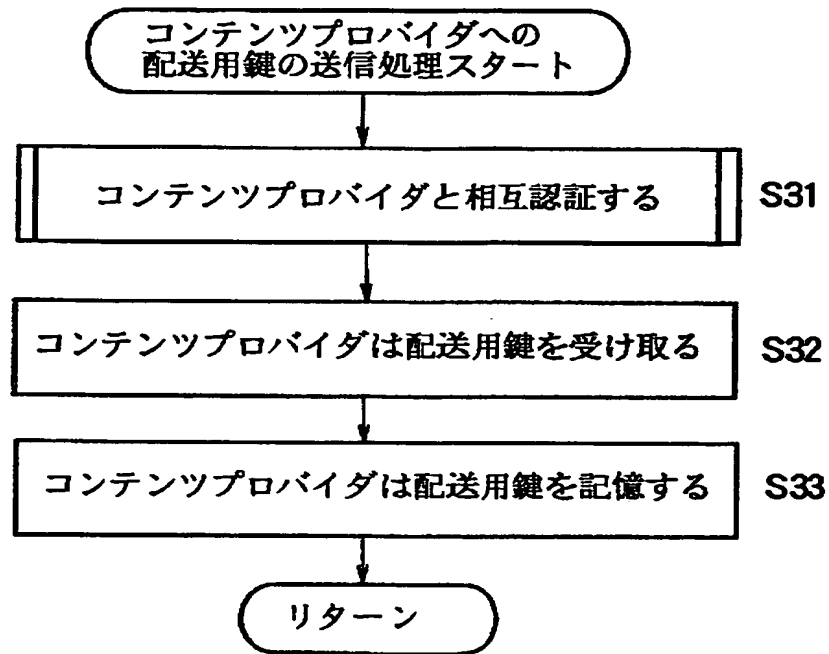
【図 30】



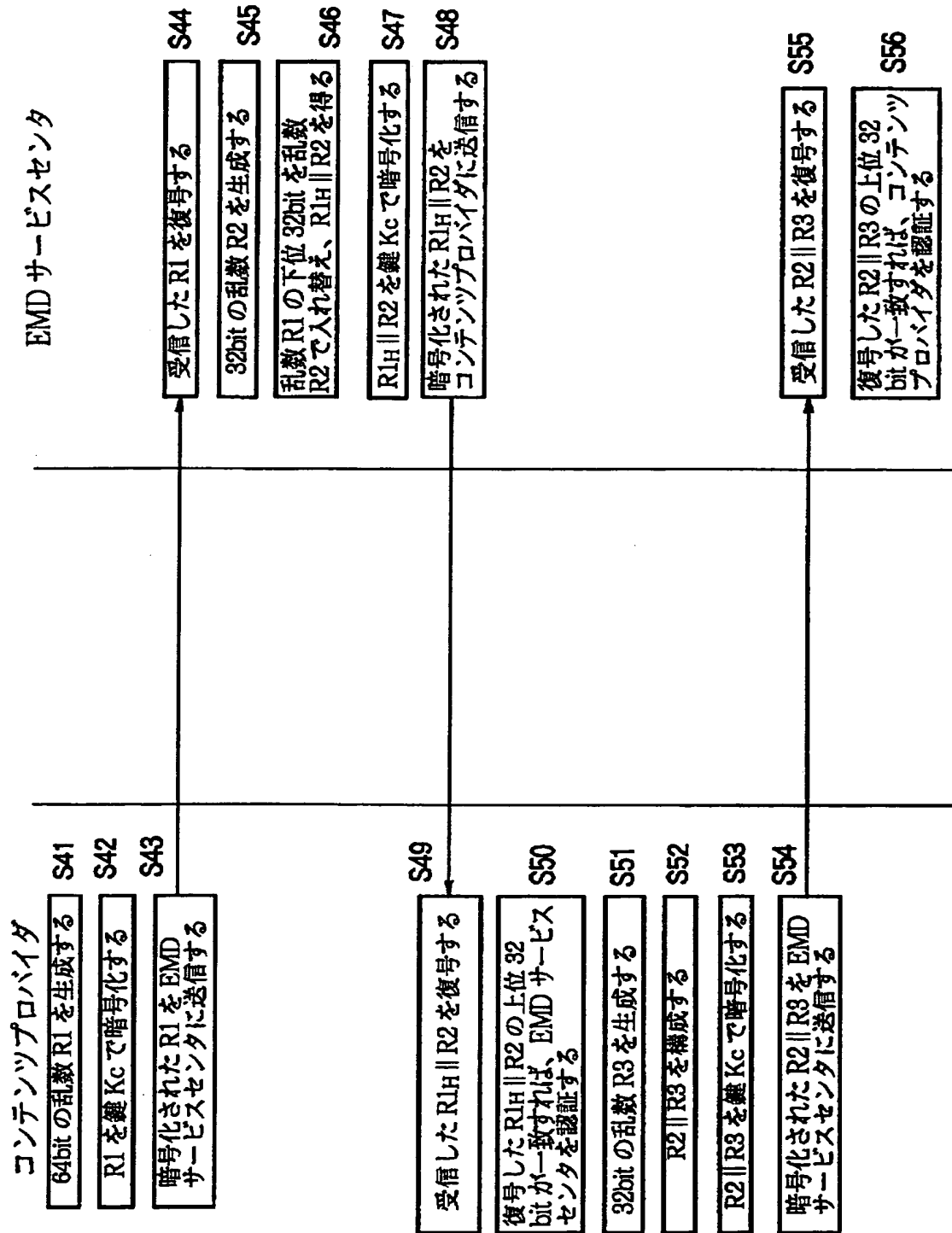
【図 31】



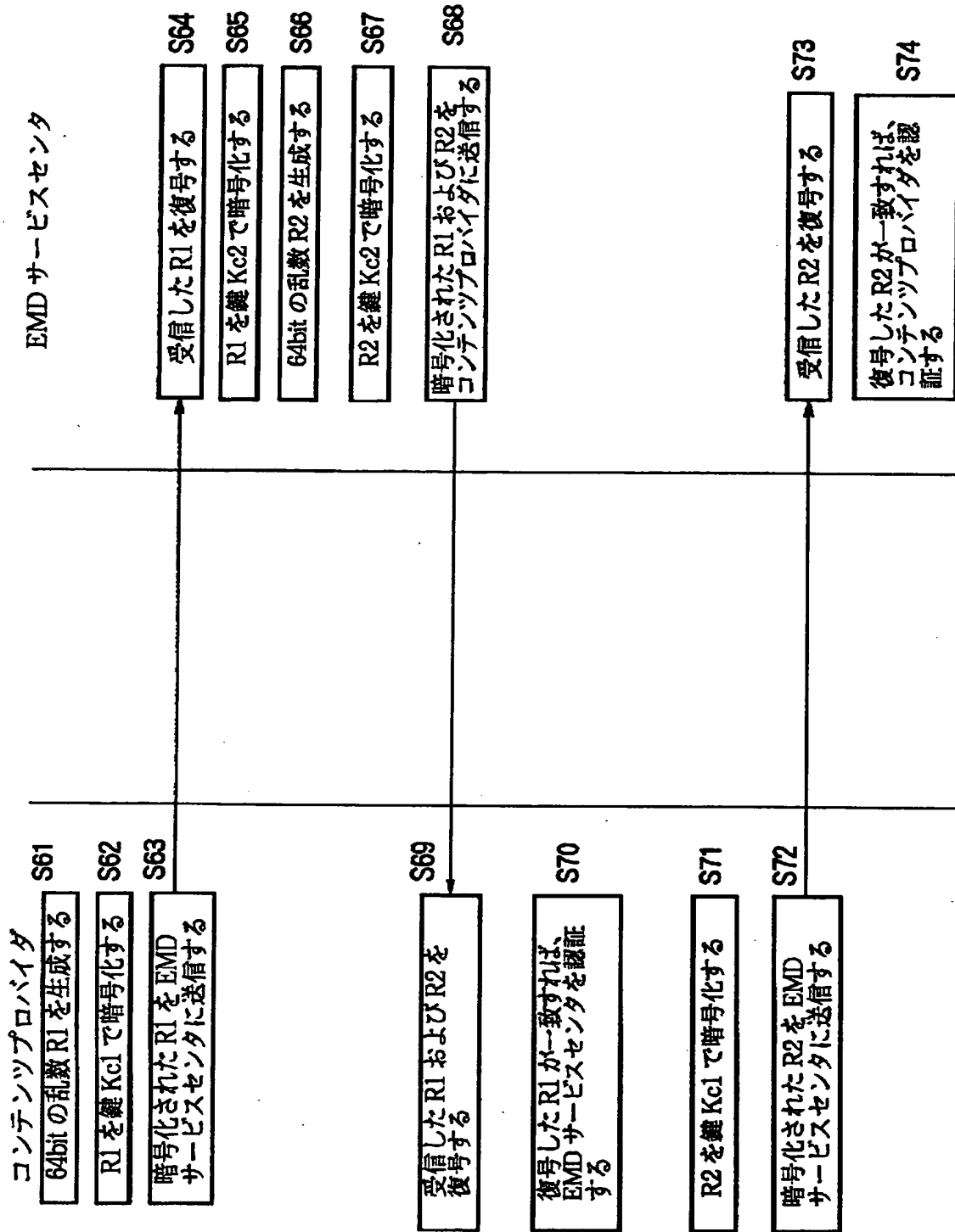
【図 3 2】



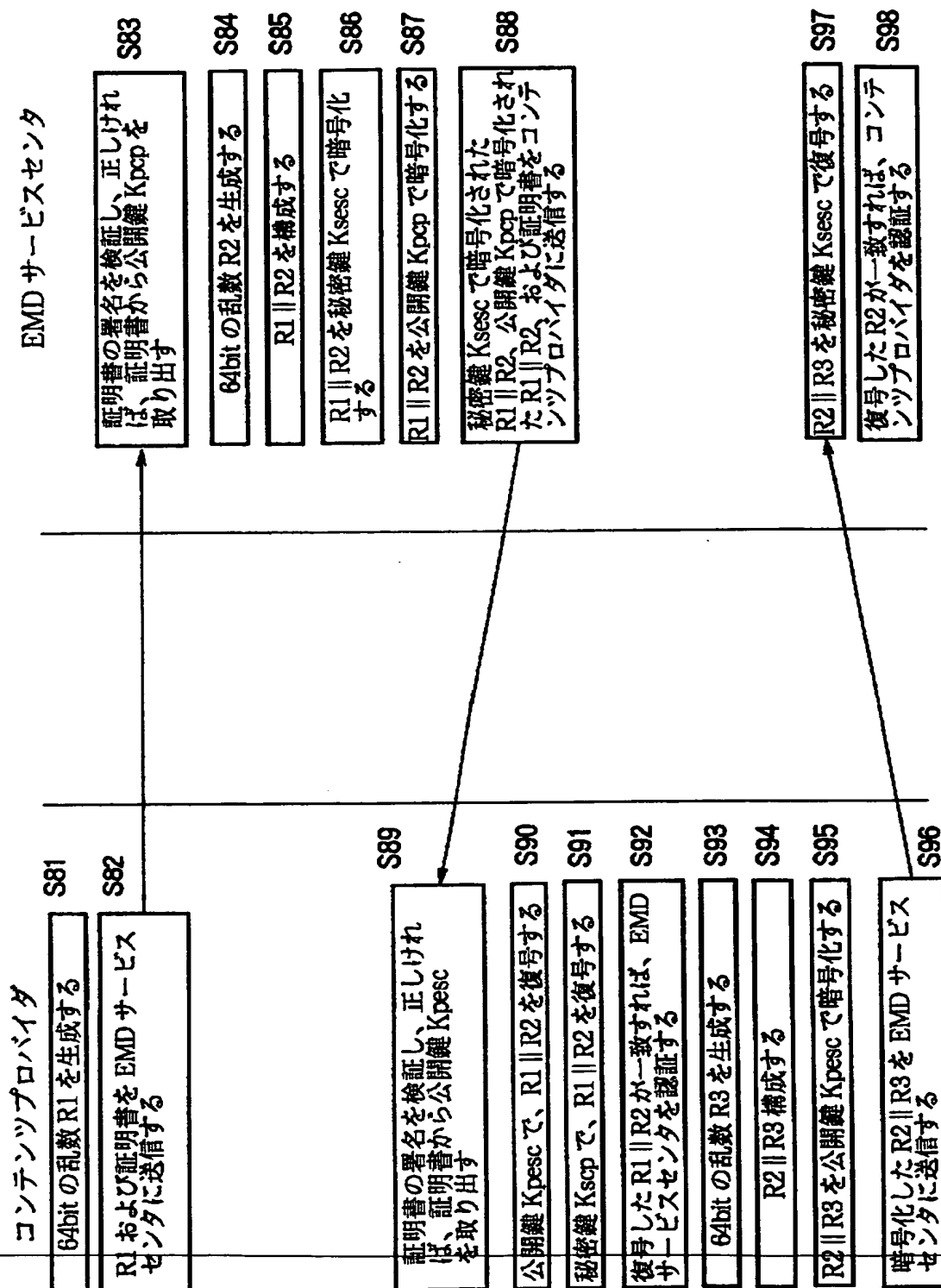
【図 3 3】



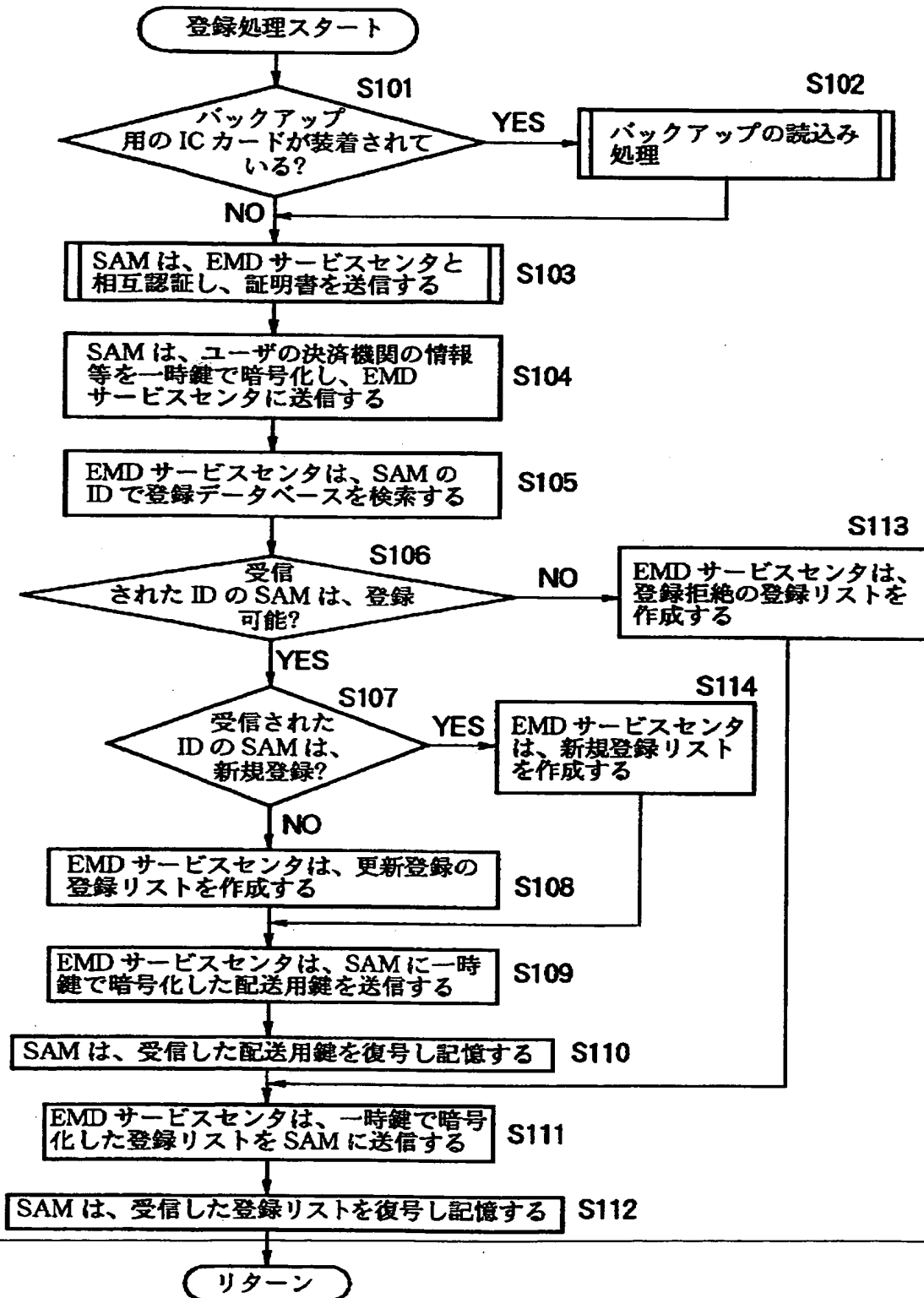
【図 3 4】



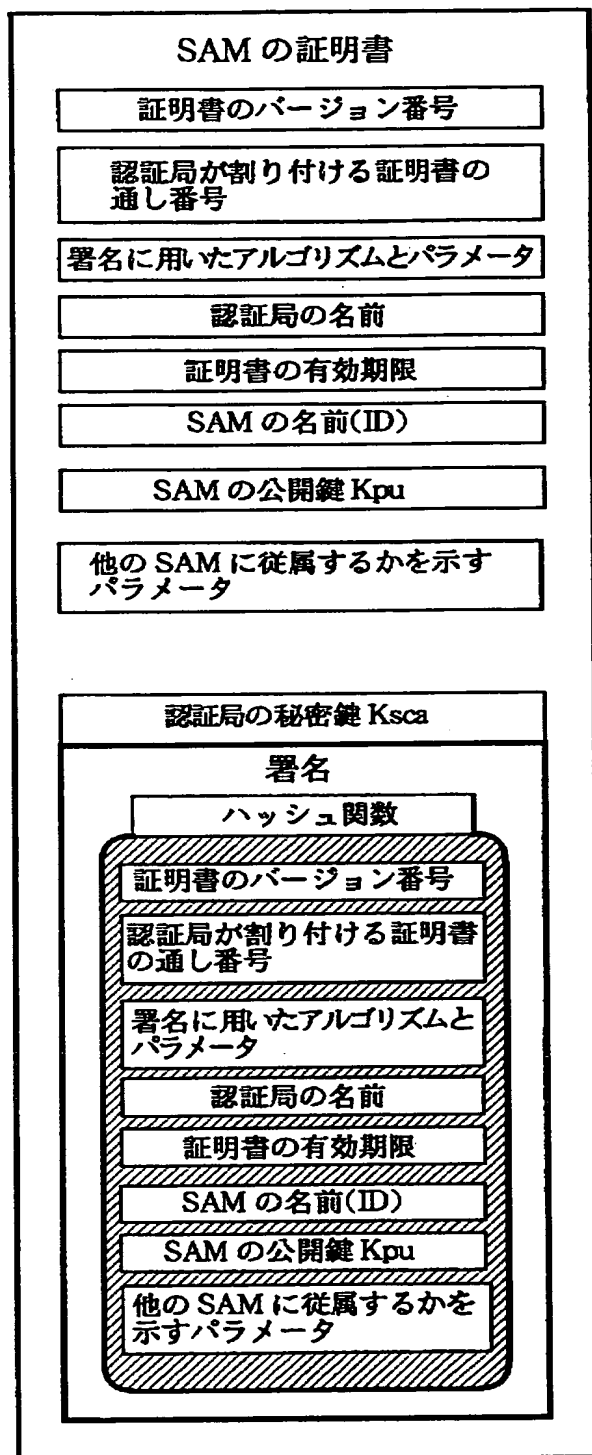
【図 3 5】



【図 3 6】



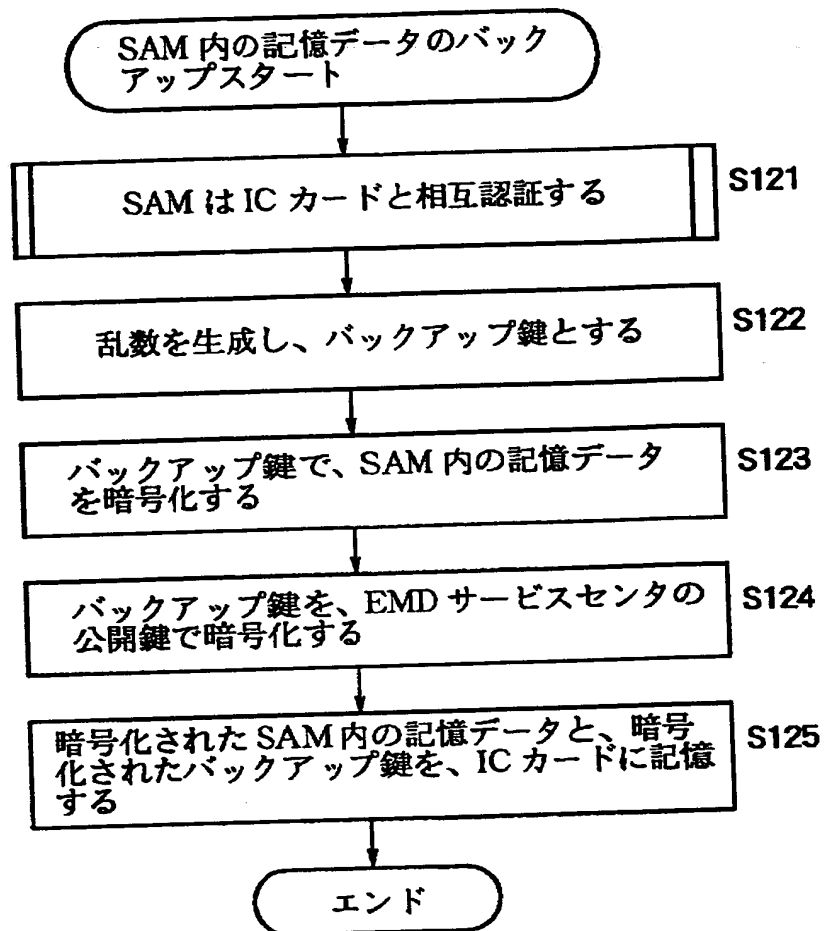
【図 37】



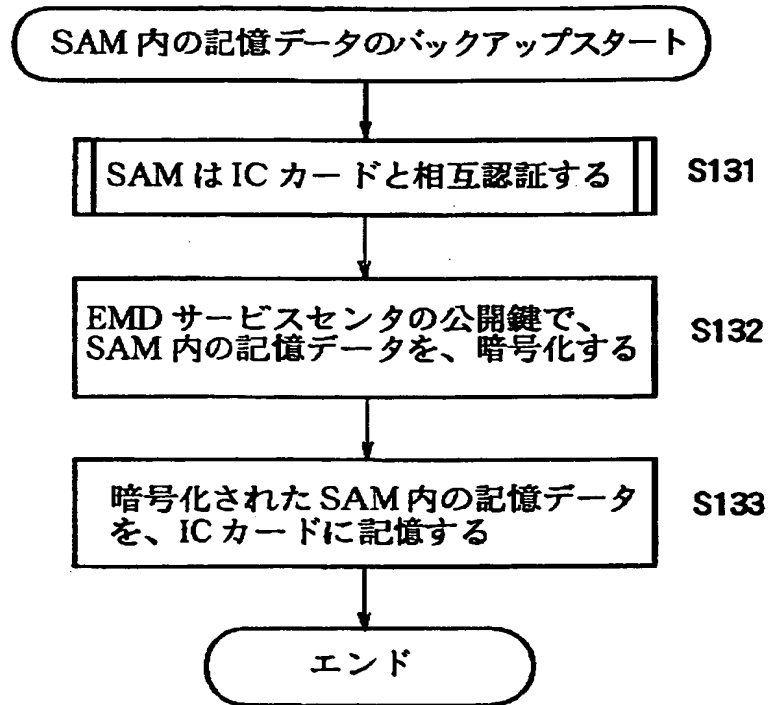
【図 3 8】

SAM の ID (64bit)	登録拒絶フラグ (1bit)	ステータスフラグ (4bit)	コンディションフラグ (1bit)	署名
00000000000000000001h	1	0000	0	XXXXXXXXXX
00000000000000000002h	1	1010	1	XXXXXXXXXX
00000000000000000003h	1	1100	1	XXXXXXXXXX
0000000000000000000Ah	0	0000	1	XXXXXXXXXX

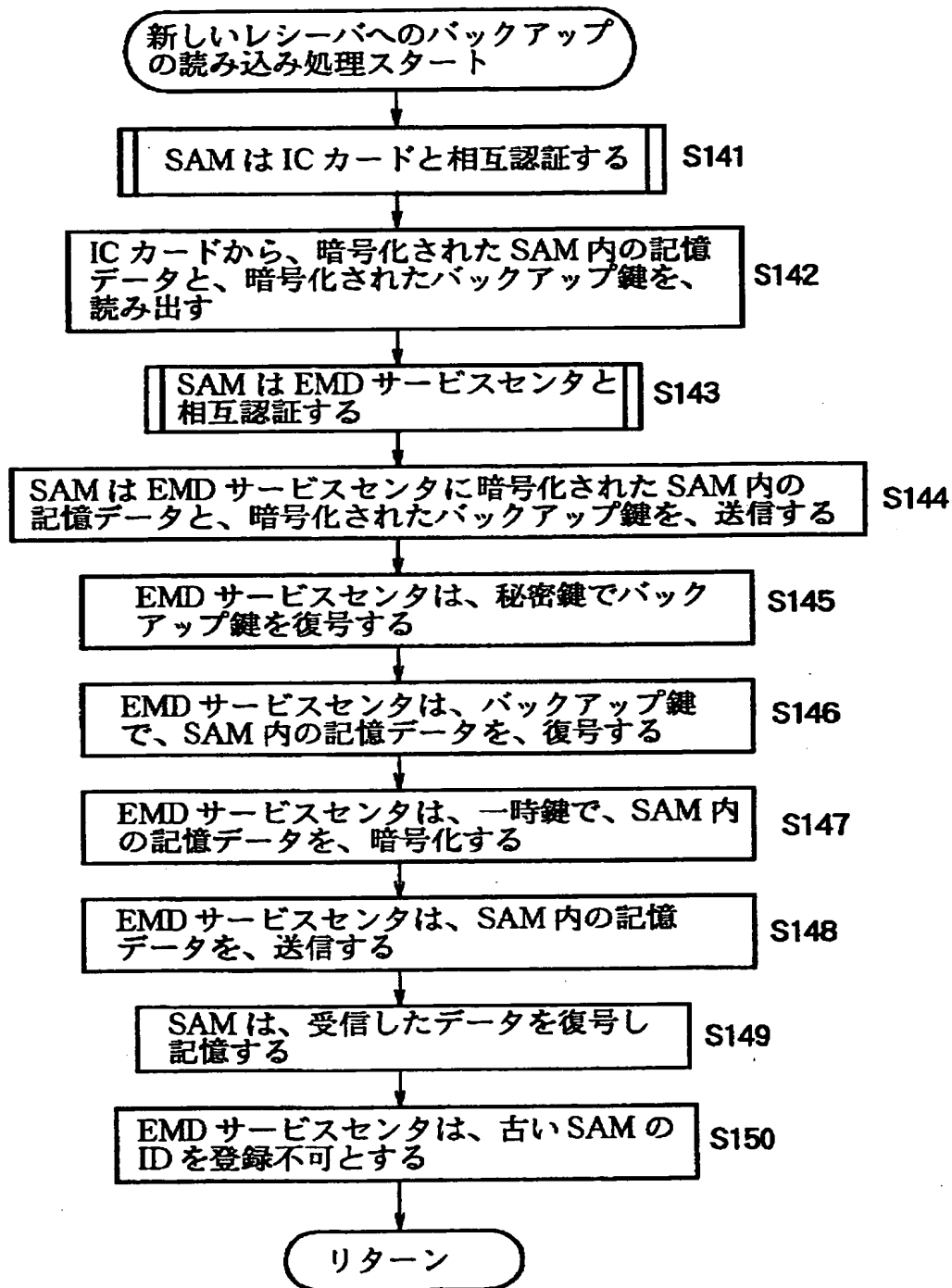
【図 39】



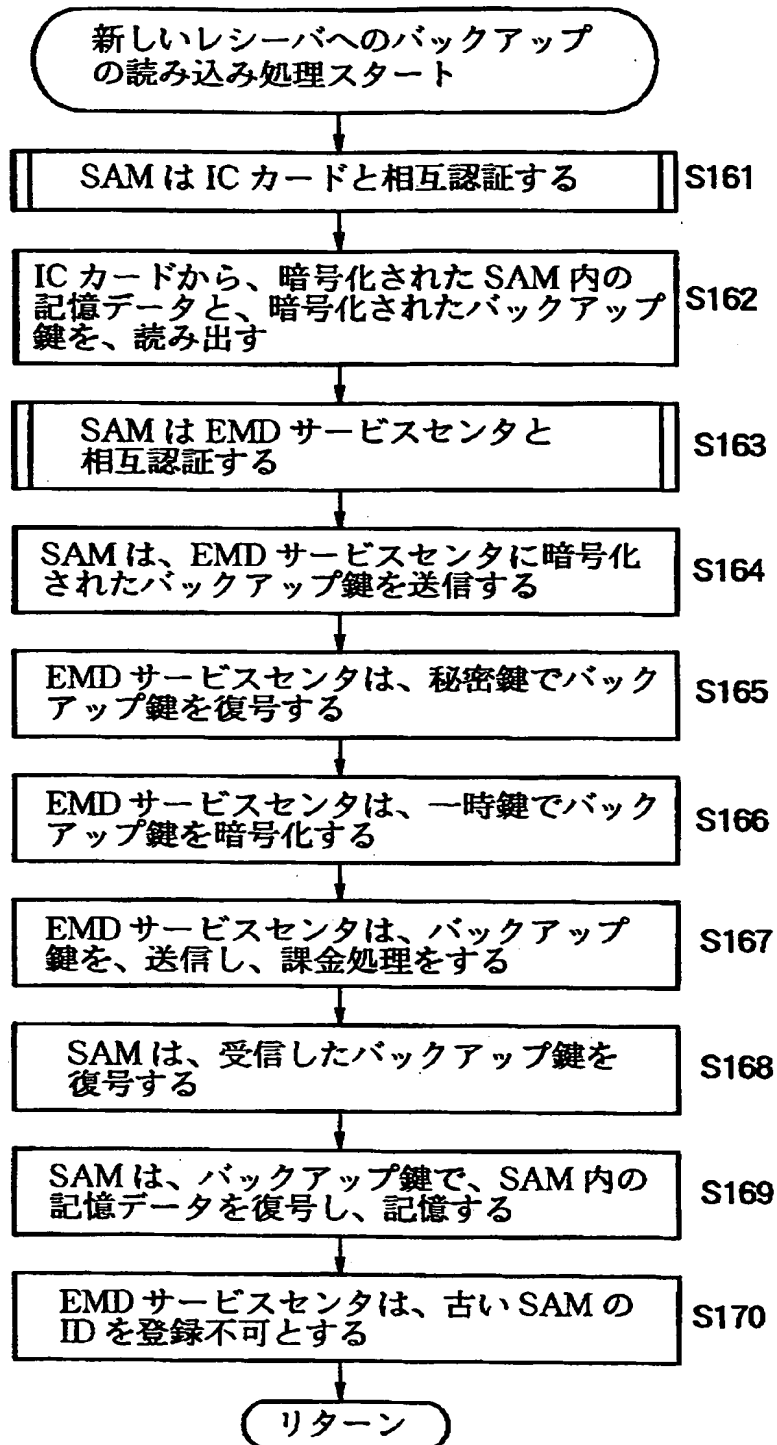
【図 40】



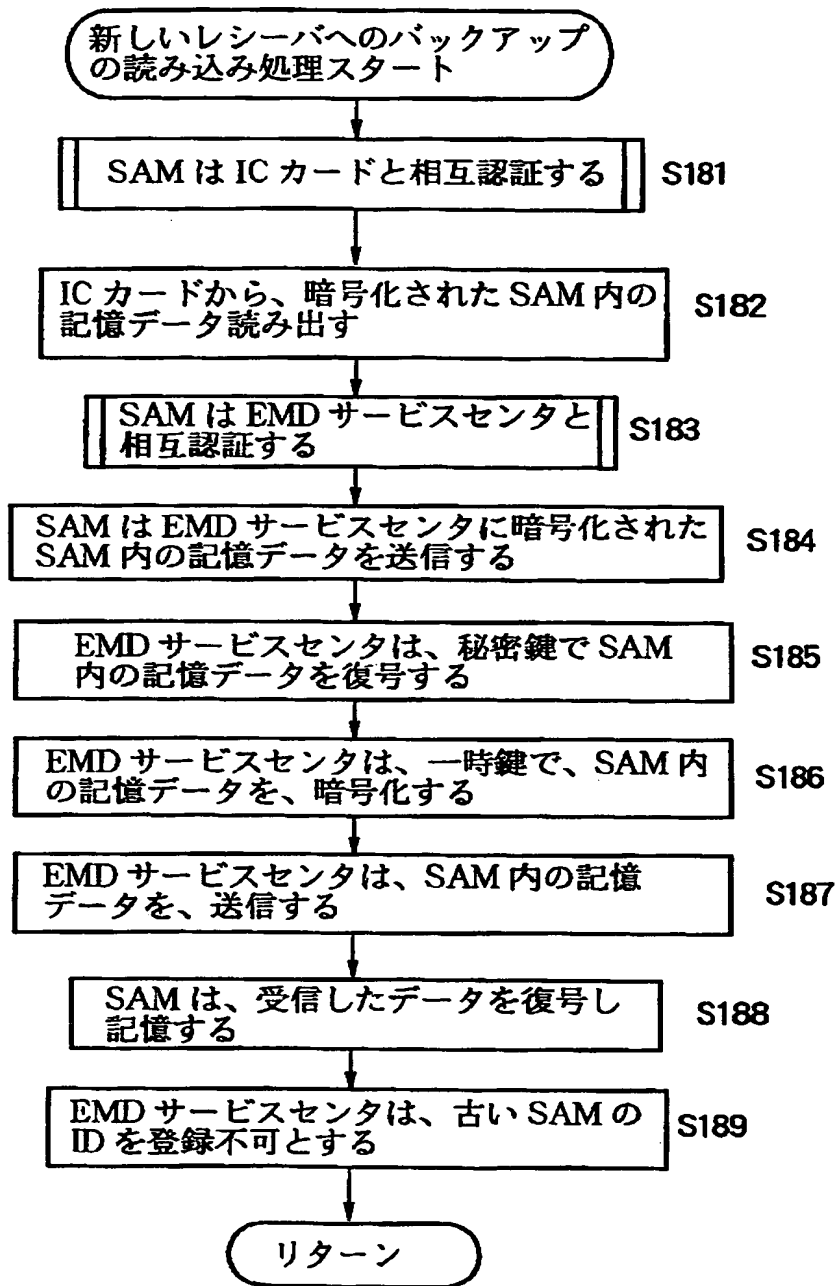
【図 4 1】



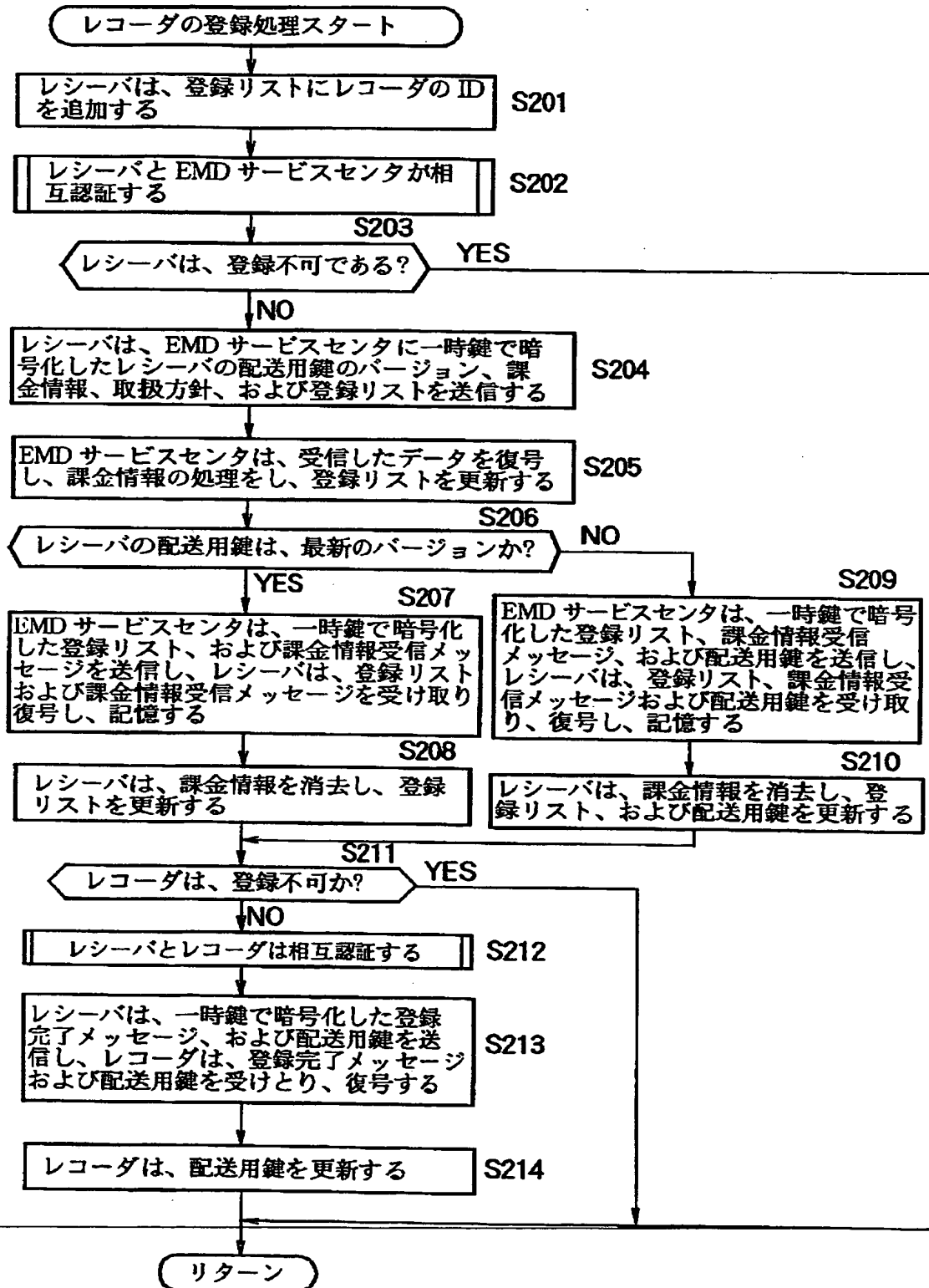
【図 4 2】



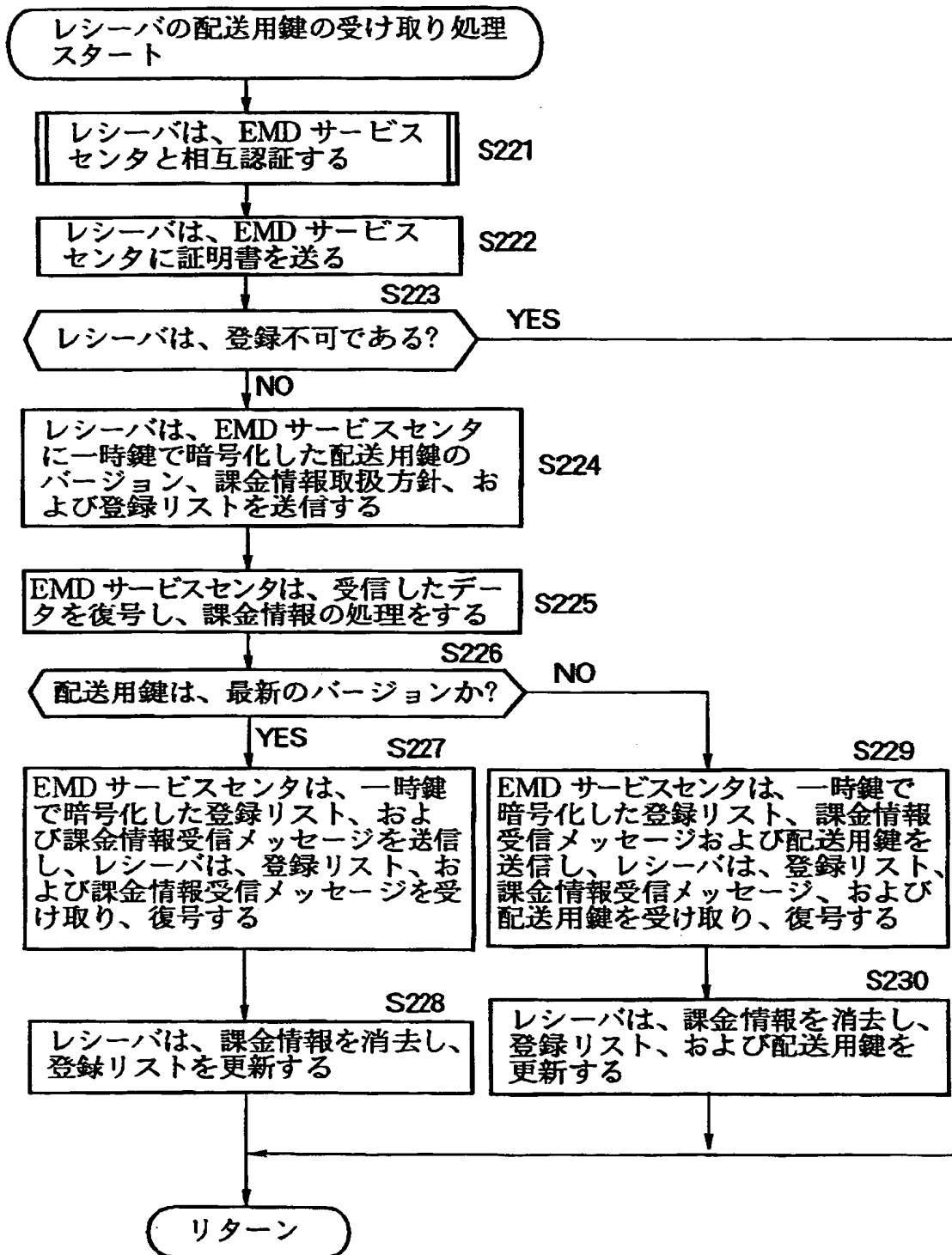
【図 4 3】



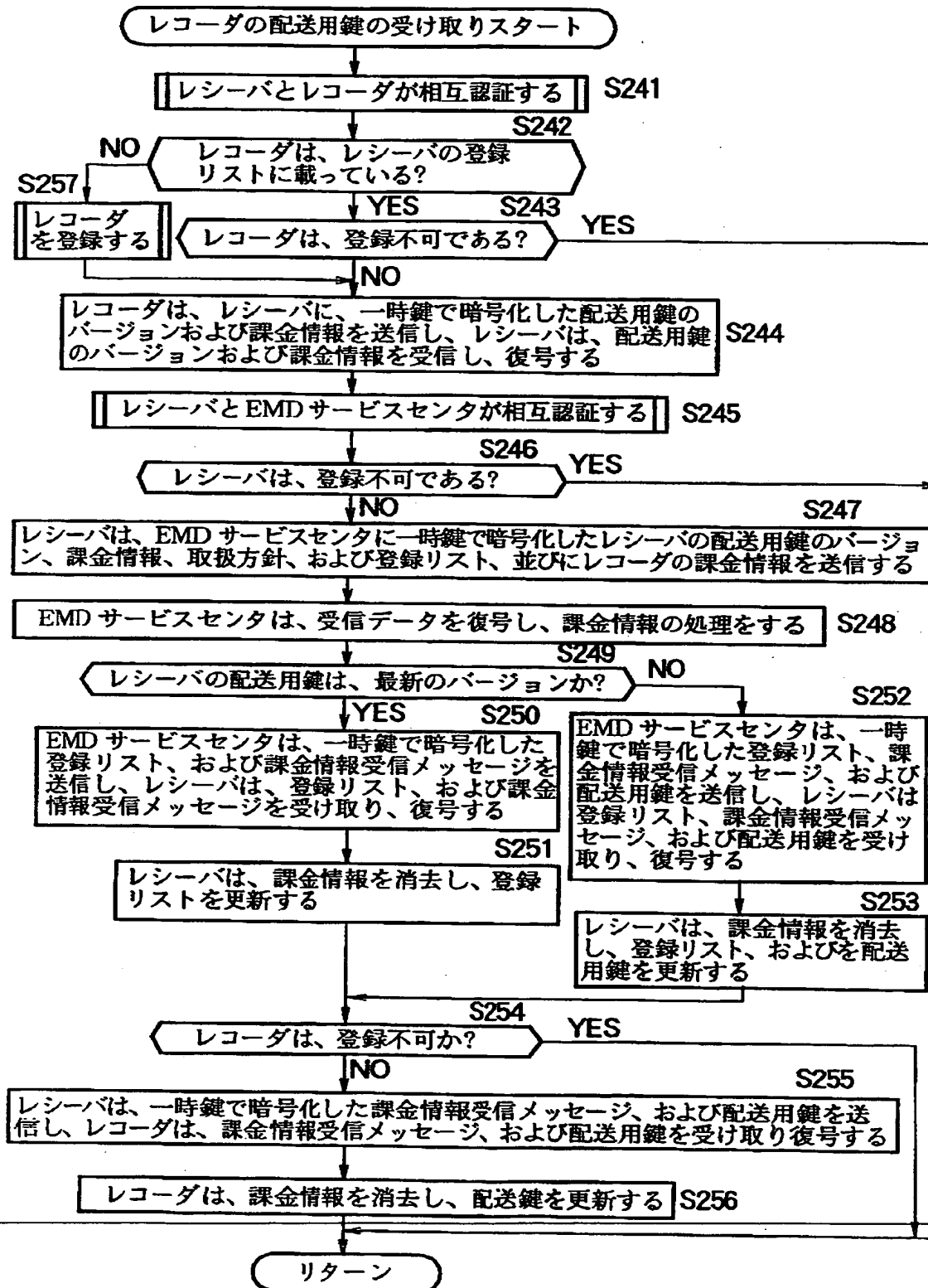
【図 4 4】



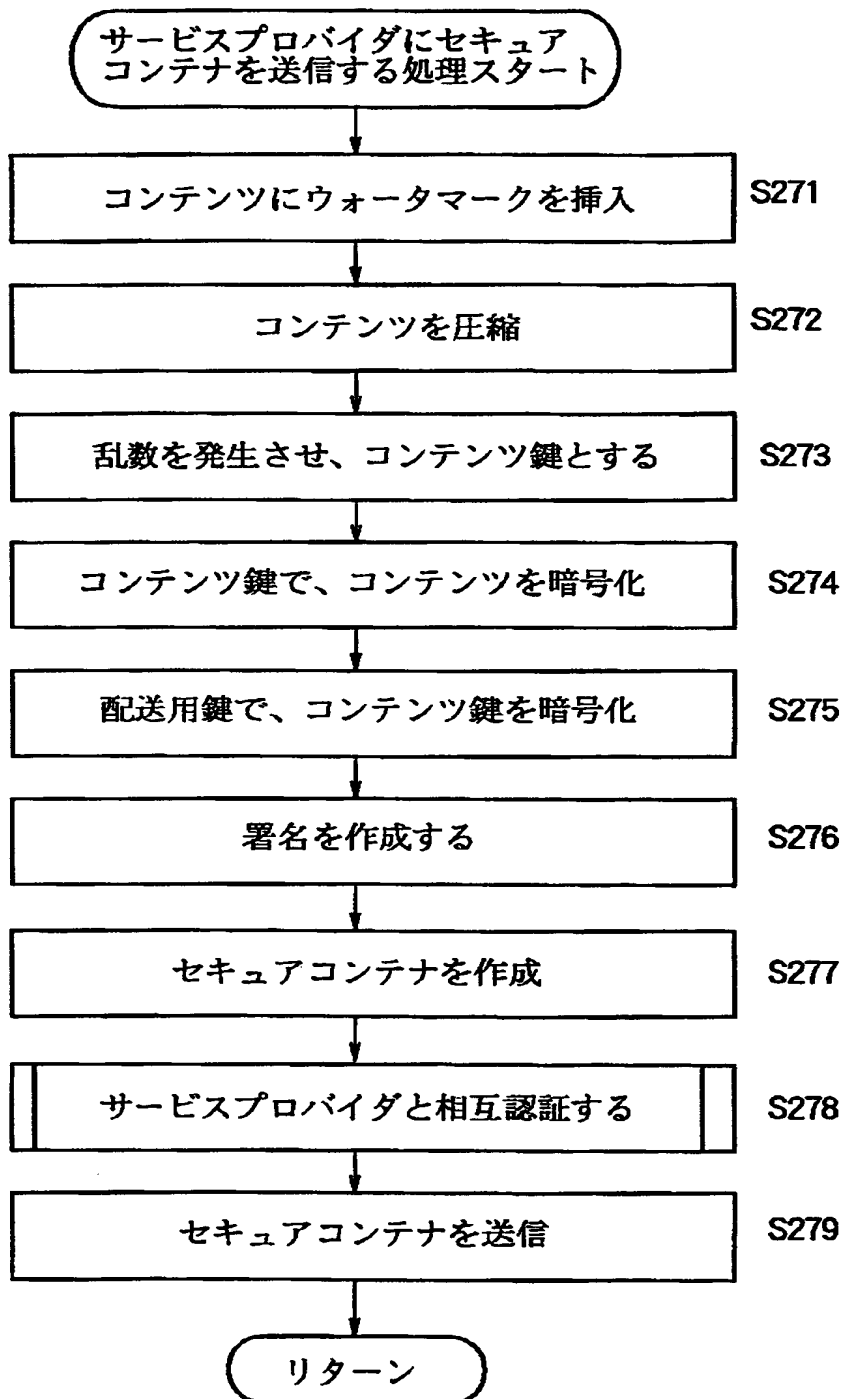
【図 4 5】



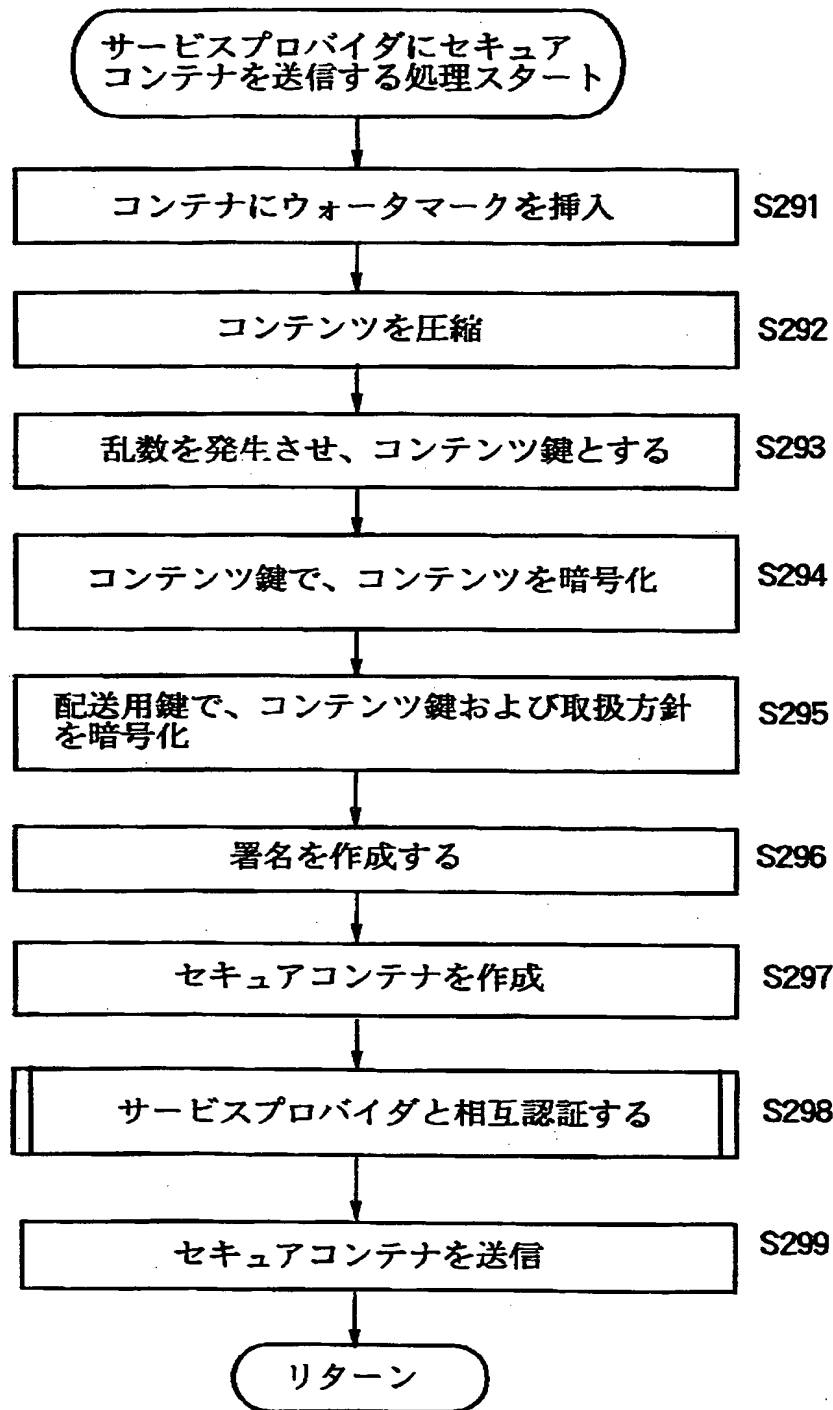
【図 4 6】



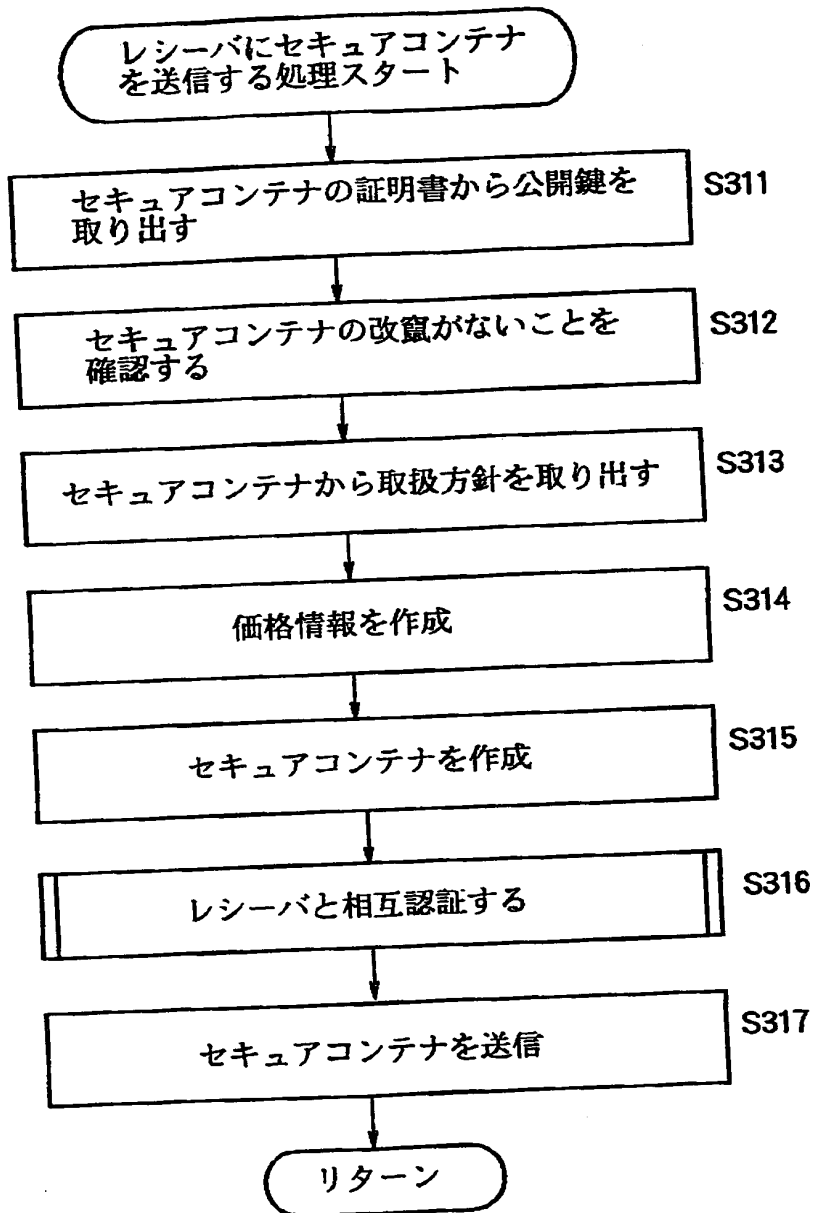
【図 47】



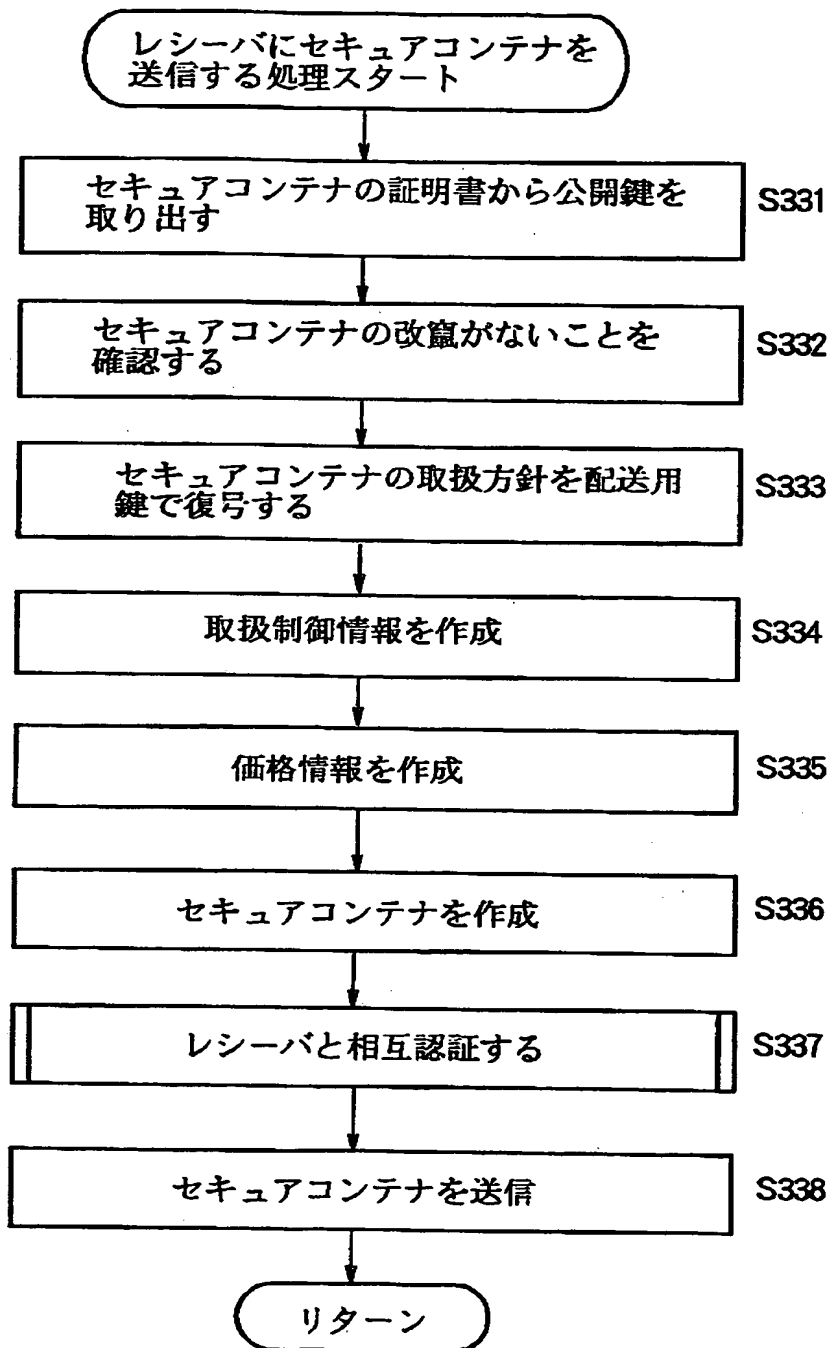
【図 48】



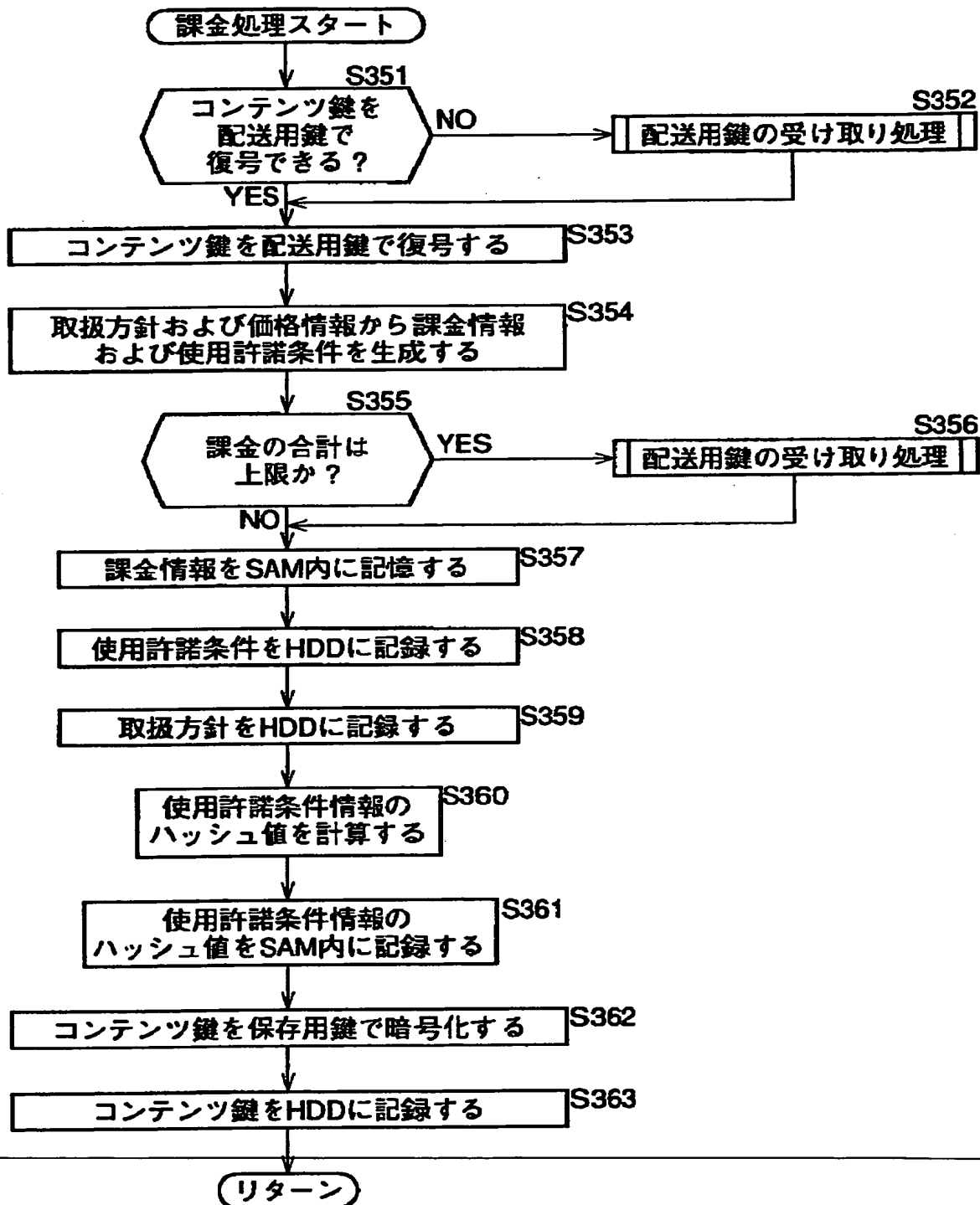
【図 49】



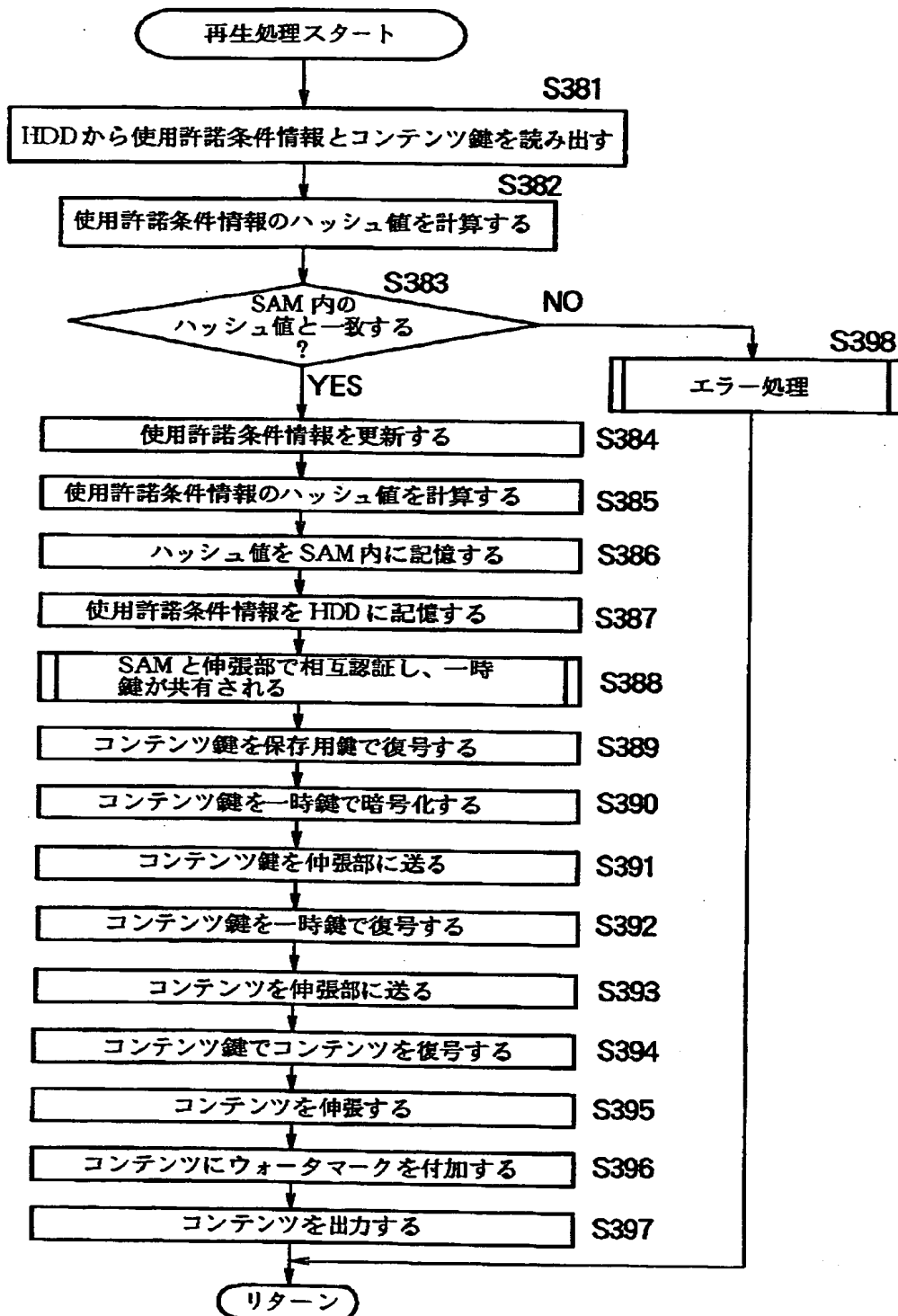
【図 50】



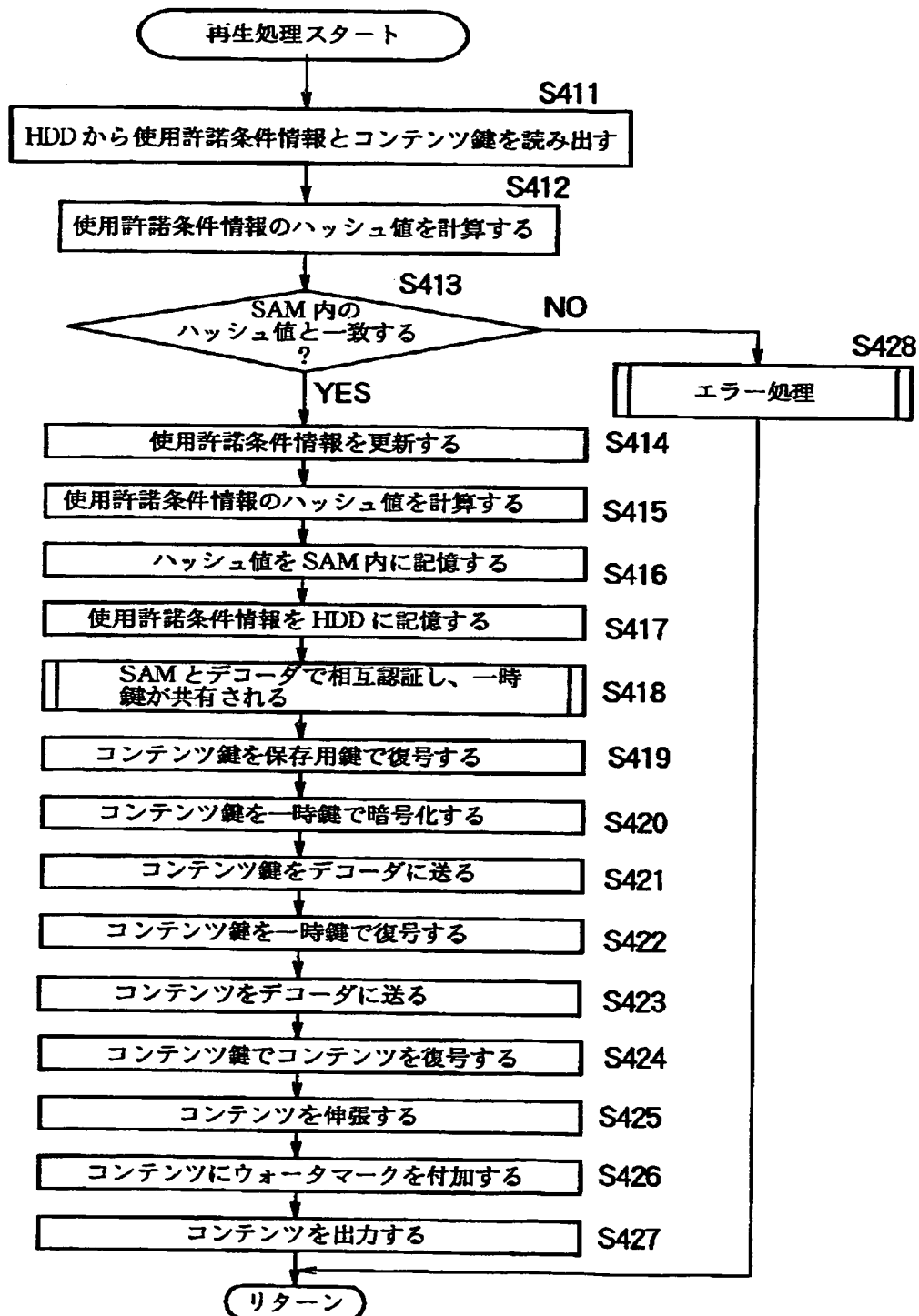
【図 51】



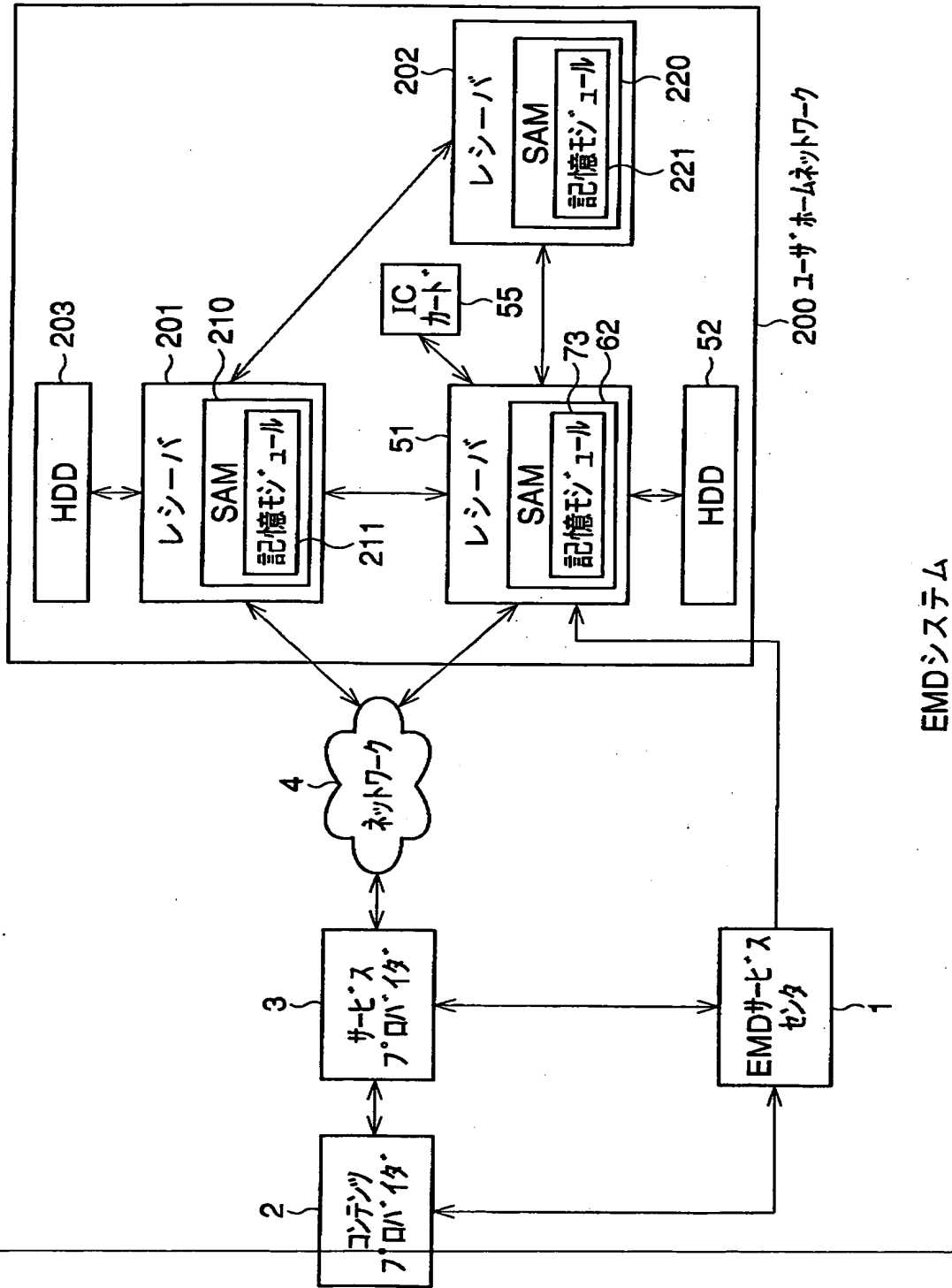
【図 5 2】



【図 53】



【図54】



【図55】

リスト部							
SAM ID	ユーザ ID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態情報	登録条件署名
レジバ51の登録条件 SAM62のID	ユーザのID	可	可	SAM62のID	なし	制限なし	XXXX
レジバ201の登録条件 SAM210のID	ユーザのID	可	不可	SAM62のID	なし	制限なし	XXX
レジバ202の登録条件 SAM220のID	ユーザのID	不可	不可	なし	SAM62のID SAM210のID	制限なし	XXX

対象SAM情報部	
対象SAMID	SAM62のID
有効期限	XXXX
バージョン番号	XXXX
接続されている機器数	
3	

レジバ51の登録リスト

特平 11-103337

【図56】

リスト部							
SAM ID	ユーザ ID	購入 処理	課金 処理	課金 機器	コンテンツ 供給機器	状態 情報	登録条件 署名
SAM62の ID	ユーザのID	可	可	SAM62 のID	なし	制限 なし	XXXX
SAM210の ID	ユーザのID	可	不可	SAM62 のID	なし	制限 なし	XXX
SAM220の ID	ユーザのID	不可	不可	なし	SAM62の ID SAM210の ID	制限 なし	XXX

バージョン 51 の
登録条件

バージョン 201 の
登録条件

バージョン 202 の
登録条件

対象SAMID	SAM210のID
有効期限	XXXX
バージョン番号	XXXX
接続されている機器数	3

対象SAM
情報部

バージョン 201 の登録リスト

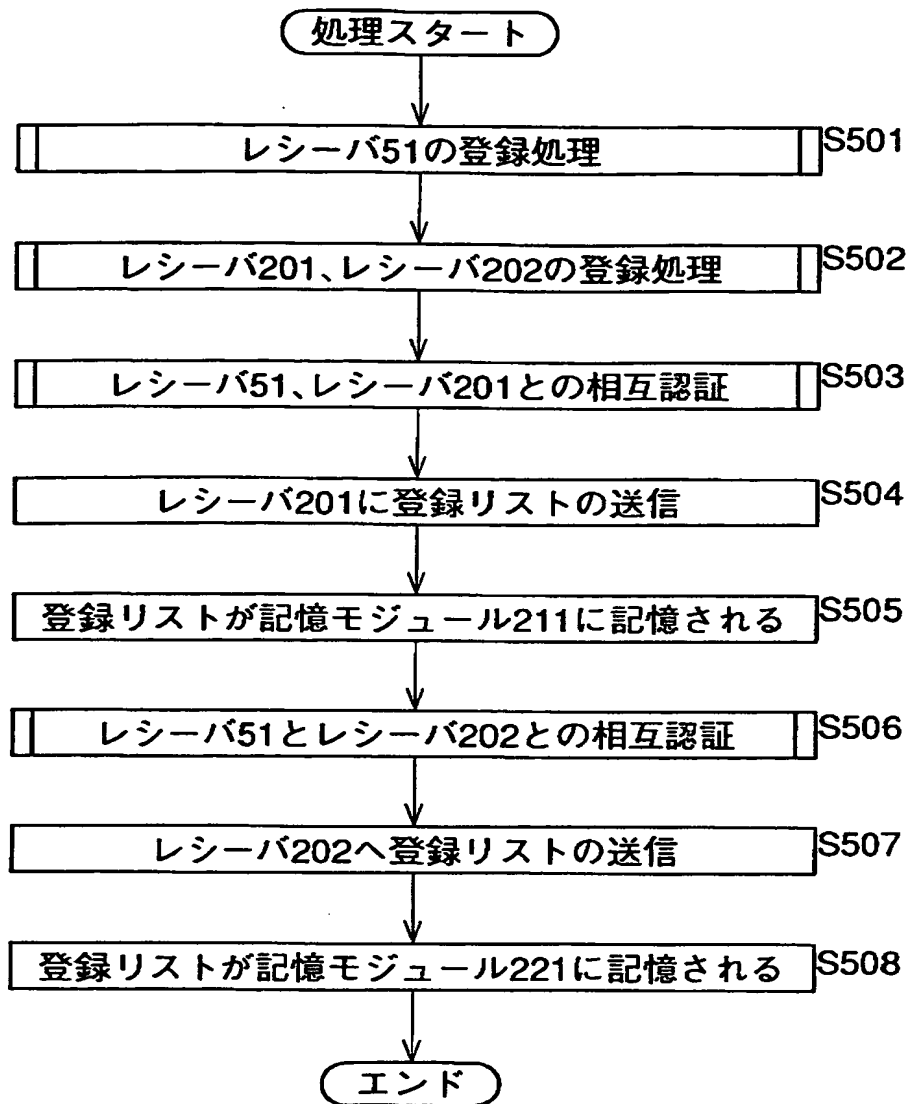
【図57】

レシーバ202の登録条件		リスト部				
SAM ID	ユーザID	購入処理	課金処理	課金機器	コンテツ供給機器	状態情報
SAM220のID	ユーザのID	不可	不可	なし	SAM62のID SAM210のID	制限なし
						登録条件 署名 XXX
						登録リスト 署名 XXXX

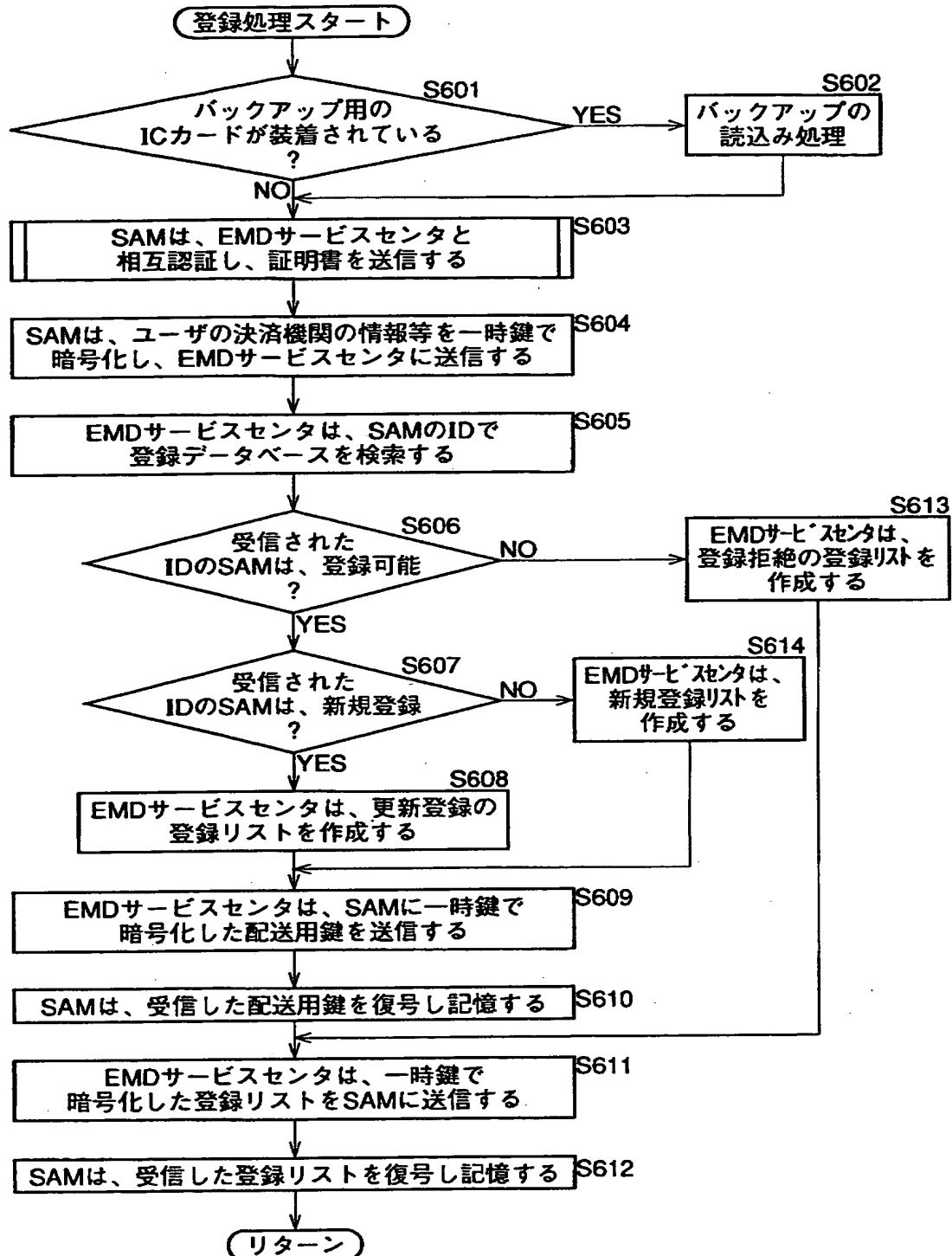
対象SAMID	SAM220のID	対象SAM情報部
有効期限	XXXX	XXXX
バージョン番号	XXXX	XXXX
接続されている機器数	3	

レシーバ202の登録リスト

【図58】



【図59】



【図60】

リスト部

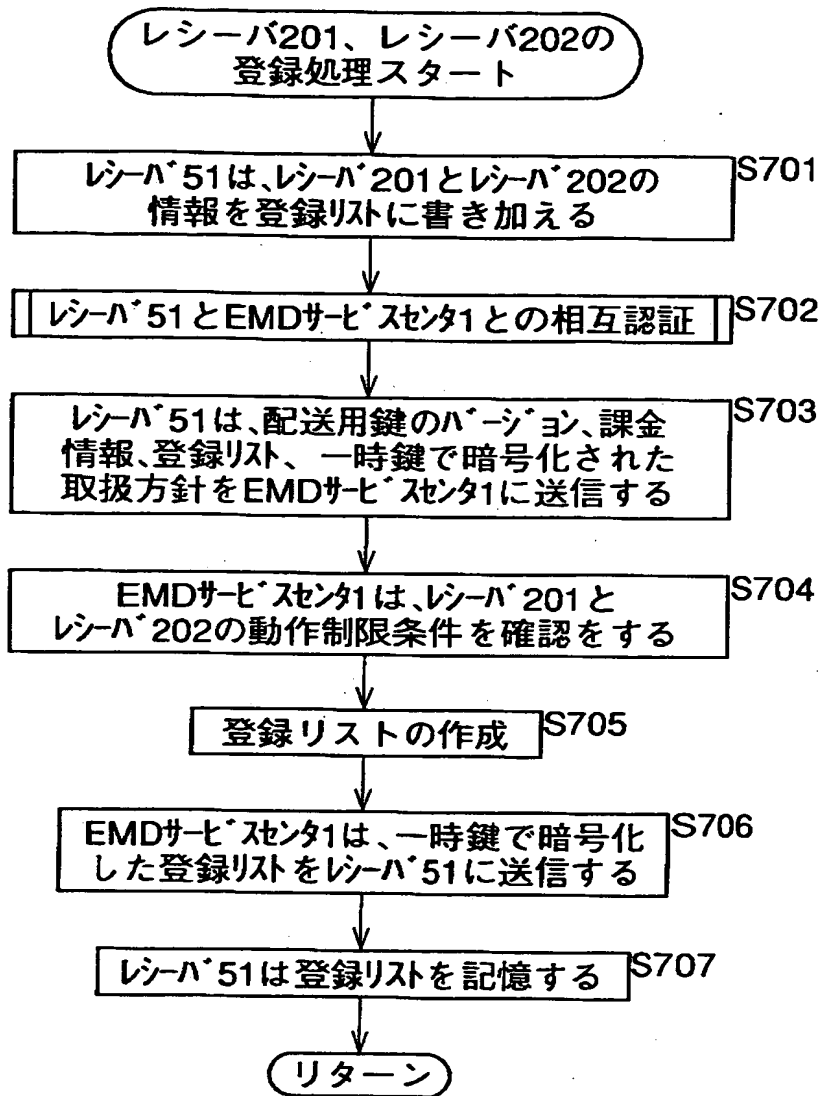
SAM ID	ユーザ・ID	購入 処理	課金 処理	課金 機器	コンデジツ 供給機器	状態 情報	登録条件 署名	登録リスト 署名
SAM62の ID	ユーザ・のID	可	可	SAM62の ID	なし	制限 なし	XXX	XXXX

ユーザ51の
登録条件

対象SAM 情報部	
対象SAMID	SAM62のID
有効期限	XXXX
バージョン番号	XXXX
接続されている機器数	
3	

登録リスト

【図61】



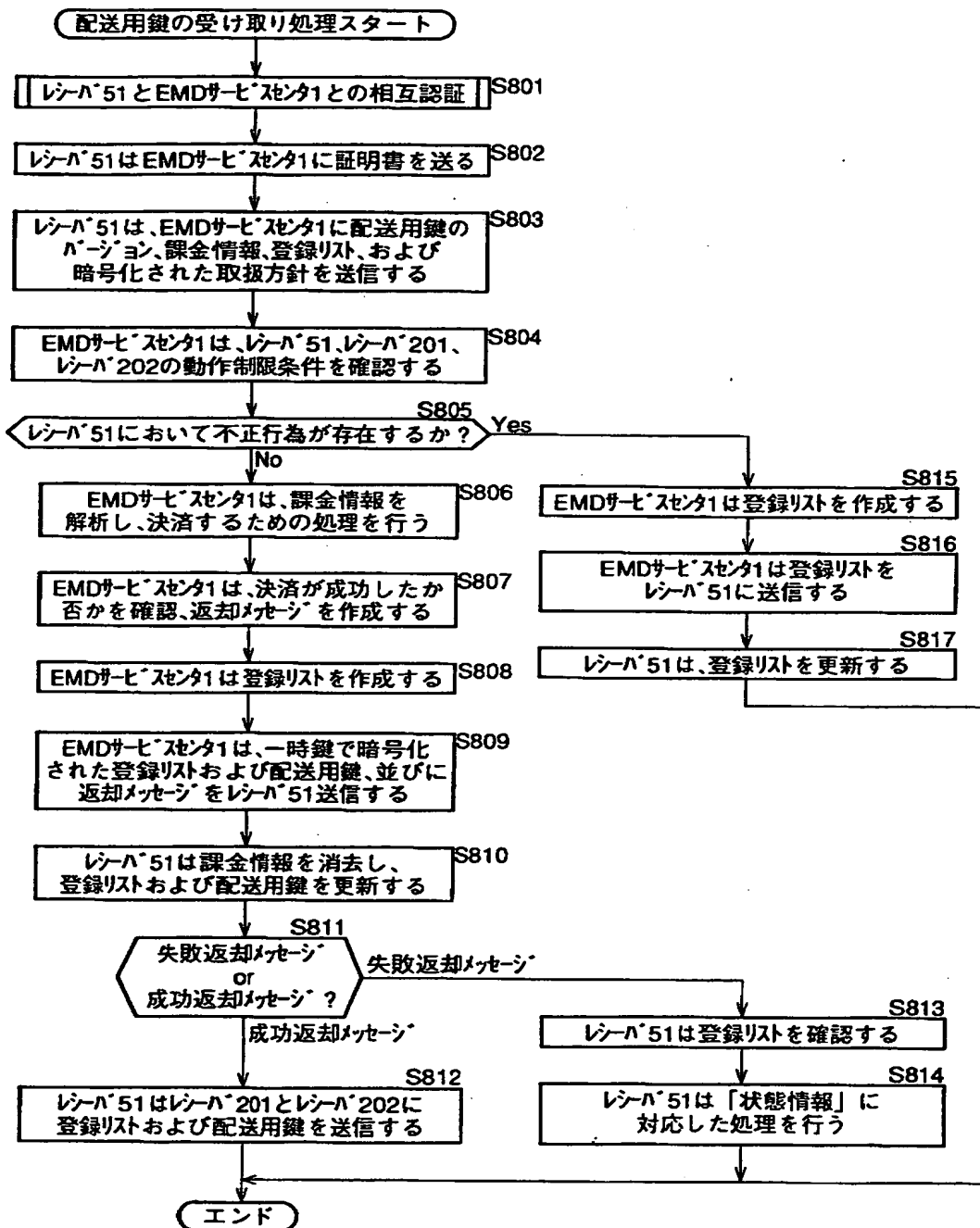
【図62】

リスト部						
SAM ID	ユーザ ID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態情報
SAM62のID	ユーザのID	可	可	SAM62のID	なし	制限なし
SAM210のID		可	不可	SAM62のID	なし	制限なし
SAM220のID		不可	不可	なし	SAM62のID SAM210のID	制限なし
						登録条件署名
						登録条件署名
						登録条件署名

レシーバ51の登録条件

対象SAM情報部	
対象SAMID	SAM62のID
有効期限	XXXX
バージョン番号	XXXX
接続されている機器数	3

【図63】



特平 11-103337

【書類名】 要約書

【要約】

【課題】 EMDシステムに登録された機器に、違反があったか否かを容易に確認することができる。

【解決手段】 EMDシステムに登録された各機器は、登録リストを保持する。例えば、課金処理が成功しなかった場合、その機器の登録リストの「状態情報」には、“制限あり”が設定される。この場合、その機器においては、すでに購入されたコンテンツの利用処理は実行されるが、新たなコンテンツを購入するための処理は実行されなくなる。また、その機器において、違反行為が発覚した場合、その機器の登録リストの「状態情報」には、“停止”が設定され、機器の動作が停止される。

【選択図】 図 5 5

認定・付加情報

特許出願の番号	平成11年 特許願 第103337号
受付番号	59900339685
書類名	特許願
担当官	第八担当上席 0097
作成日	平成11年 4月15日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川6丁目7番35号
【氏名又は名称】	ソニー株式会社

【代理人】

申請人	
【識別番号】	100082131
【住所又は居所】	東京都新宿区西新宿7丁目5番8号 GOWA西 新宿ビル6F 稲本国際特許事務所
【氏名又は名称】	稲本 義雄

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社